Digitaler Service Public

Studie im Auftrag des BAKOM

Thomas Gees, Daniel Hürlimann, Reinhard Riedl, Matthias Stürmer, Flurina Wäspi

Bern, 3.05.2022

Berner Fachhochschule
Departement Wirtschaft
Institut Public Sector Transformation

Inhaltsverzeichnis

Management Summary

Der vorliegende Bericht entstand im Auftrag des Bundesamts für Kommunikation (BAKOM). Das Institut Public Sector Transformation am Departement Wirtschaft der Berner Fachhochschule (BFH) hat zu Beginn des Jahres 2022 eine Studie erarbeitet, ausgehend vom Postulat 19.3574 (Postulat Min Li Marti) zur Zukunft eines digitalen Service Public (DSP) in der Schweiz. Welche Grundversorgungleistungen sind denkbar, wo könnten für den Staat neue Aufgaben in der Grundversorgung eines digitalen Service Public entstehen, welche neu zu schaffenden Infrastrukturen sind im öffentlichen Interesse? Der im Zug der Digitalisierung sich weiter entwickelnde Service Public in den herkömmlichen Bereichen (etwa Post, öffentlicher Verkehr, Gesundheit) wurde hingegen nicht untersucht. Das Interesse liegt auf neuen Herausforderungen im Bereich Daten, Netzwerke und Software. Ausserdem umfasst der Bericht eine Einschätzung zu rechtlichen Fragen und diskutiert das Konzept «Government as a Platform (GaaP)».

Der Bericht behandelt neue, noch wenig systematisch untersuchte Fragen. Er zeigt auf, wo sich in der Einschätzung der Verfassenden staatliches Handeln als notwendig erweisen dürfte. Der Staat kann in Bezug auf digitale Güter, Services und Infrastrukturen entweder als Anbieter oder als Regulator handeln, er kann aber auch private Angebote als gemeinwirtschaftliche Aufgabe fördern. Ausgehend von den ökonomischen Überlegungen zum Marktversagen als Rechtfertigung für staatliches Handeln zur Kompensation von Wohlfahrtsverlusten wurde ein Framework für einen Digitalen Service Public entwickelt. Denn anders als bei den herkömmlichen Infrastrukturen (Telekommunikation, Verkehr, Medien etc.) liegt die gesellschaftspolitische Herausforderung einer digitalen Grundversorgung weniger an einem fehlenden privaten Angebot, sondern vielmehr an den Bedingungen für die Nutzung des Angebots, welche die Anbieter aufgrund ihrer oft umfassenden Marktmacht stellen können. Das Framework definiert drei Situationen, unter welchen Bedingungen staatliches Handeln erforderlich ist:

1. Es gibt keinen Anbieter auf dem Markt, sodass ein gesellschaftlich erwünschtes Gut nicht produziert wird.
2. Individuen oder der Staat sind bei einem bestehenden Angebot hohen Abhängigkeiten von privaten Anbietern ausgesetzt.
3. Das Vertrauen in einen Dienst ist nicht gegeben, weil zum Beispiel die Nutzerinnen und Nutzer ihre persönlichen Daten weitergeben müssen.

Um das Phänomen Digitalisierung bezüglich der technologischen Ausprägung strukturell besser zu erfassen, wurde das Technologieschichtenmodell der Deutschen Akademie der Technikwissenschaften (acatech) herangezogen. Dieses wurde zwar für die Beurteilung der digitalen Souveränität in Europa und der Bundesrepublik Deutschland entwickelt, ist aber für die vorliegende Studie wertvoll, wenn die Digitalisierung als mehrschichtige technologische Erscheinung (z.B. Kommunikationsinfrastrukturen, Datenräume oder Softwaretechnologien) verstanden wird.

Zusammenfassend ist der Staat für einen zukünftigen digitalen Service Public in diesen Gebieten gefragt:

- Aufbau von sektorspezifischen Datenräumen (Infrastruktur und Governance), welche das Datenteilen und die Datenvalorisierung fördern und eine zukünftige Einbindung in europäische Datenräume antizipieren
- Konsequentes Bereitstellen der staatlichen und halbstaatlichen Daten auf einer zentralen Plattform für offene Verwaltungsdaten
- Digitale Basisinfrastruktur für Cloud-Services, um der Abhängigkeit von Hyperscalern zu entgehen (wobei die genaue Rolle des Staates noch zu klären ist)
- Das Problem des Vendor Lock-in bei Clouddiensten führt zu hohen switching costs, hier muss die Schweiz ebenfalls beobachten, wie die europäischen Regulierungen (etwa der Data Act) Wirkung erzielen.
- Der Staat sollte die Entwicklung von Open Source Software (OSS) fördern, indem er sich an internationalen Initiativen beteiligt, welche allfällige Sicherheitslücken überwachen.
- Um bei aussergewöhnlichen Ereignissen (z.B. Pandemien oder Naturkatastrophen) das Datenpotenzial besser zu nutzen, sollte die Schweiz Zugang auch zu privaten Daten einfordern können.
- Ungedeckte Kosten entstehen bei zahlreichen privaten Initiativen im Bereich der energiesparsamen Datenübertragung, z.B. «Long Range Wide Area Networks» (LoRaWAN); diese Kosten könnte der Staat übernehmen.
- Kooperativ sollte sich der Staat gegenüber privaten Initiativen wie Open Street Map verhalten.

Diskutiert werden auch die aus den Grundrechten abgeleiteten staatlichen Schutzpflichten im Zug der Digitalisierung. Hier macht der Bericht zahlreiche Vorschläge (etwa zum besseren Schutz der Meinungs- und Informationsfreiheit, zur Privatsphäre und zur Wirtschaftsfreiheit, zum Recht auf Teilhabe am wissenschaftlichen Fortschritt).

Das Konzept «Government as a Platform» ist für den Staat als Treiber der Digitalisierung interessant, weil es einerseits als normative Vorstellung die soziale Teilhabe am Internet als Vertrauensraum einschliesst, und anderseits vielfältige praktische Lösungsansätze beinhaltet, welche die digitale Transformation beschleunigen. Zur Grundversorgung im digitalen Raum gehört, dass sich Menschen und Unternehmen digital vertrauenswürdig ausweisen können. Es wird ein staatlich verankertes, aber von Staat, Wirtschaft und Zivilgesellschaft gemeinsam zu bauendes eID-Ökosystem empfohlen. Dieses kann mit Self Sovereign Identities (SSI) so realisiert werden, dass es mit dem entstehenden eID-Ökosystem der EU kompatibel ist.

1. Auftrag, Ausgangslage, Status quo

Das Bundesamt für Kommunikation (BAKOM) hat das Institut Public Sector Transformation der Berner Fachhochschule, Departement Wirtschaft, Ende Dezember 2021 beauftragt, einen Bericht zum Postulat 19.3574 (Postulat Min Li Marti) über den digitalen Service Public (DSP) in der Schweiz zu verfassen. Der vorliegende Bericht zuhanden des BAKOM deckt nicht die gesamte Fragestellung des Postulats Marti ab; er konzentriert sich primär auf die komplett neuen durch die Digitalisierung entstehenden möglichen Ansprüche einer Grundversorgung von Diensten (Services), technologischen Infrastrukturen sowie den Zugang zu *Daten*[1] von öffentlichem Interesse. Die bestehenden Service Public-Angebote, die physischen Infrastrukturen (Spitäler, Verkehrsnetz, Telekommunikationsnetz, etc.) werden hingegen nicht beleuchtet.[2]

Kapitel 1 klärt den Auftrag und diskutiert die Problematik Digitaler Service Public unter besonderer Berücksichtigung der Eigenschaften digitaler Güter. Dieser Bericht spricht von möglichen Veränderungen in der (staatlichen) Grundversorgung und problematisiert die möglichen Herausforderungen einer Unterversorgung von digitaler Infrastruktur oder Diensten, was auch immer die Ursachen dafür. Im Abschnitt 1.1 werden die Begrifflichkeiten geklärt. An dieser Stelle weisen wir auf die teilweise synonym verwendeten und daher unscharfen Begriffe «Grundversorgung», «Service Public» oder «Daseinsvorsorge» hin. Es macht im Kontext eines von einer staatlichen Organisation in Auftrag gegeben Berichts Sinn, der offiziellen Logik des letzten Berichts des Bundesrats zu folgen:

> «Service Public umfasst eine politisch definierte Grundversorgung mit Infrastrukturgütern und -dienstleistungen, welche für alle Bevölkerungsschichten und Regionen des Landes nach gleichen Grundsätzen in guter Qualität und zu angemessenen Preisen zur Verfügung stehen sollen.» [3]

Wie die Definition klar macht, handelt es sich letztlich um ein normatives, ein politisch zu klärendes Konzept, das in der Schweiz entweder als Service Public oder auch als Grundversorgung umschrieben wird. In Deutschland hat sich der Begriff der Daseinsvorsorge etabliert. Klassischerweise wird der Service Public im Sinne der Grundversorgung als Infrastrukturleistung dort verstanden, wo Leistungen gesellschaftlich erwünscht, aber vom Markt nur unvollkommen oder gar nicht bereitgestellt werden (näher im folgenden Abschnitt 1.1.1). Wie bereits der Bericht des Bundesrates von 2004 zur Grundversorgung in der Infrastruktur zur weiteren Entwicklung festgehalten hat, führt der «technologische Fortschritt (…) zur Existenz neuer Dienstleistungen und ermöglicht, traditionelle Dienstleistungen auf neue Weise zu erbringen (z.B. elektronischer Postverkehr, Telefonieren über das Internet, Radio und Fernsehen via Internet usw.)». Der Bericht von damals war ganz der Liberalisierungsprozesse der 1980er und 1990er Jahre verpflichtet, wo es um die Entkoppelung der Dienstleistung (des «Service») vom Dienstleistungserbringer (öffentliches Unternehmen oder Verwaltung) ging. Der Staat fand sich nach der Liberalisierung vermehrt in der Rolle des Regulierers

[1] Kursiv gedruckte Begriffe finden sich im Glossar am Ende des Berichtes wieder. Das Glossar stützt sich dabei unter anderem auf die Begriffsdefinitionen im kürzlich veröffentlichten Bericht des BAKOM zur Förderung vertrauenswürdiger Datenräume (UVEK und EDA 2022)

[2] Eine Ausnahme bildet Abschnitt 1.3 mit den Rechtsgrundlagen des bestehenden Service Public.

[3] Bericht des Bundesrates (23.06.2004) «Grundversorgung in der Infrastruktur (Service Public)», https://www.newsd.admin.ch/newsd/message/attachments/9238.pdf

wieder, der sicherstellen sollte , dass der «Service Public» erbracht wird (Finger, 2021). Dafür – so Finger – haben sich die Begriffe «Gewährleistungsstaat», die Terminologien «Public Service Obligation» (oder «PSO») und «Universaldienst» («Universal Service Obligation») eingebürgert.[4]

In diesem Bericht geht es nicht um die Fortsetzung der Grundversorgungsproblematik in den bisherigen öffentlichen Sektoren, welche sich infolge digitaler Innovationen weiterentwickelt haben. Der Bericht thematisiert generell, mit welcher Unterversorgung oder unzureichenden Art und Weise der Versorgung die Gesellschaft infolge der digitalen Transformation von Netzwerken, Daten und Software konfrontiert ist. Anders als bei den Netzwerkinfrastrukturen der Vergangenheit, stellt sich weniger die Frage, warum es keine Versorgung gibt, obwohl diese im öffentlichen Interesse wäre (Marktversagen), sondern ob die Versorgung durch bereits bestehende Anbieter laufend gesellschaftlich unerwünschte Risiken produziert, und welche Versorgung der Staat alternativ zu Privaten anbieten sollte. Deshalb wird auch aufgezeigt, an welchen Wertvorstellungen sich ein Digitaler Service Public (DSP) orientieren sollte bzw. wie ein Digitaler Service Public zu legitimieren ist.

1.1 Public Goods und digitale Güter: Theorie und Framework

1.1.1 Eigenschaften digitaler Güter

Dass der Markt nicht immer die zufriedenstellende Allokation von Gütern und Dienstleistungen hervorbringt, ist in der ökonomischen Theorie immer wieder beschrieben worden. Wenn eine Marktlösung für ein (sozial) erwünschtes Gut entweder gar nicht bereitgestellt wird oder «Marktversagen» oder «Marktunvollkommenheiten» vorliegen, dann ist die sogenannte allokative Effizienz der Ressourcen nicht gegeben. Üblicherweise beschreibt die standardökonomische Theorie eine Unterbereitstellung öffentlicher Güter, wobei neben dem Verlangen nach der staatlichen Allokation von Gütern und Dienstleistungen (also, damit die Gesellschaft überhaupt ein Angebot erhält bzw. dass dieses optimal bereitgestellt wird), auch weitere Überlegungen als legitim gelten. So wird häufig auch die Verteilungsgerechtigkeit genannt. Dieses Argument ist allerdings ein normatives, weshalb sich die standardökonomische Theorie schwertut, ein Optimum zu ermitteln.

Im OECD-Raum oder innerhalb der Europäischen Union ist der Anspruch auf eine staatliche Grundversorgung[5] in der Verfassung und anderen Gesetzen festgelegt, sodass die Bevölkerung einen Anspruch auf Dienste/Infrastrukturen oder Güter hat. Dieser Anspruch legt deshalb auch fest, dass weniger vermögende Menschen eine Versorgung mit Energie, Abwasser und Abfallbeseitigung, aber auch Telekommunikation sowie eine Gesundheitsversorgung in Anspruch nehmen können (Mause, 2018). Die Etablierung des Service Public kann man zwar nicht auf den Wohlfahrstaat der Nachkriegszeit

[4] Die zentrale Referenz in diesem Zusammenhang ist die sogenannte "PSO Regulation" der Europäischen Union von 2007, die sich jedoch zum damaligen Zeitpunkt ausschliesslich auf den Personentransport auf Schiene und Strasse bezog: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32007R1370; seither hat sich der Term "Public Service Obligation" in allen netzbasierten Industrien etabliert, ausser im Post- und Telekomsektoren, wo, stattdessen, der Begriff Universaldienst (oder präziser "Universal Service Obligation") verwendet wird.

[5] In den USA und Australien werden öffentlich bereitgestellte Dienstleistungen wie beispielsweise Energie oder Wasser- ver- und -entsorgung «universal service (obligations)» genannt, in Grossbritannien spricht man vom «public service» beziehungsweise «services of general economic interest», während in Frankreich vom «Service Public» oder «service d`intérêt général» die Rede ist. Auf der Ebene der Europäischen Union wird der Bezeichnung «Dienstleistungen von allgemeinem (wirtschaftlichen) Interesse» der Vorzug vor dem Begriff der Daseinsvorsorge gegeben (Neu (2009), S 9).

direkt zurückführen, wohl aber den starken Ausbau von Infrastrukturen als Ausdruck der Teilhabe an den gesellschaftlichen Entwicklungen im Zuge der wohlfahrtsstaatlichen Expansion. Infrastrukturpolitik war und ist somit Ausdruck für ein ausgleichendes soziales und regionales Wohlstandsniveau innerhalb der Nation. Eine Zäsur im Verständnis vom ‚sorgenden' zum ‚gewährleistenden' Wohlfahrtsstaat hat Ende der 1980er Jahre bis etwa ins Jahr 2000 stattgefunden. Konkret entwickelte sich nach Finger die «Abkoppelung der Dienstleistung vom Leistungserbringer» sowie «die Notwendigkeit, solche Dienstleistungen (ökonomisch) zu legitimieren» in der damaligen Periode (BAKOM, 2021b). Diese Entkoppelungslogik ist für eine Betrachtung einer Grundversorgung mit «digitalen Infrastrukturen und Dienstleistungen» eine wichtige Leitlinie.

Ob gemäss der Politik bestimmte Güter und Dienste in einem öffentlichen Auftrag zu erfüllen sind, entscheidet noch nicht, wer diese konkret erbringt: gemischtwirtschaftliche Unternehmen, öffentliche Unternehmen oder der private Sektor können diese Aufgabe übernehmen (Gonser & Gundlach, 2020).

1.1.2 Digitale Güter und der Service Public

Inwiefern handelt es sich bei *digitalen Gütern* um eine besondere Herausforderung für einen Service Public? Im Gegensatz zu sinkenden Grenz- und Skalenerträgen gibt es in der Plattform-Ökonomie oft gerade die umgekehrte Erscheinung, nämlich steigende Skalenerträge und Netzwerkeffekte (Bertschek et al., 2021). Die Regel, dass der Preis den Grenzkosten entspricht, gilt bei digitalen Gütern nicht. Dies führt zu Anbietern, die in kurzer Zeit den Markt beherrschen (Clement & Schreiber, 2013). Lock-in Effekte und Pfadabhängigkeiten (vgl. Abschnitt 2.5) sind die Folge. Digitale Güter weisen zudem Charakteristiken von öffentlichen Gütern auf: Die Nicht-Rivalität im Konsum etwa (Nicht-Rivalität bedeutet, dass der Konsum durch eine Person nicht die Verfügbarkeit für andere Personen verringert), oder häufig auch dass die Nutzung digitaler Güter unabhängig von der Anzahl der Nutzer ist, da die Nutzung zahlreicher Dienste und Apps kostenfrei ist. Doch stimmt das nur auf den ersten Blick; Nutzende zahlen nicht monetär, aber mit der Preisgabe ihrer Daten.

Sturn (Sturn, 2021) argumentiert, dass die Herleitung staatlicher Aufgabenerfüllung über das Marktversagen («was Private nicht machen») bei digitalen Gütern zu kurz greift. Digitale Monopole und Plattformen mit Netzwerk-Externalitäten und Lock-ins betreffen die ganze Gesellschaft, und niemand kann sich diesen privatwirtschaftlichen Angeboten entziehen. Problematisch ist deshalb nicht eine Unterbereitstellung, sondern die Macht von Monopolen in der Digitalwirtschaft, dank der Normen und Standards durchgesetzt werden (vgl. auch 2.2). Gerade weil digitale Güter Merkmale von öffentlichen Gütern aufweisen, geht die übliche ordnungspolitische Legitimation für eine staatliche Grundversorgung, bzw. für die Rolle des Staates als Produzent öffentlicher Güter, nicht auf. Aus diesem Grund haben die Verfasser dieser Studie ein Framework für einen Service Public für digitale Güter und Services entwickelt.

1.1.3 Framework für einen Service Public für digitale Güter und Services

Das Framework wurde aufgrund einer unbefriedigenden Basis in der wissenschaftlichen Literatur entwickelt. Mit dessen Hilfe soll abgeschätzt werden können, ob es einen Digitalen Service Public braucht oder nicht. Um zu beurteilen, ob der Staat seine Tätigkeit auf digitale Services ausweiten soll,

wird ein Framework vorgeschlagen, dass entlang bestimmter Kriterien angewendet werden kann. Sofern ein digitaler Service gesellschaftlich erwünscht ist, muss die Politik folgende Überlegungen berücksichtigen:

A) Gibt es bereits ein **Angebot**?
B) Existiert **Wahlfreiheit** beim bestehenden Angebot?
C) Ist das Angebot **vertrauenswürdig**?

A) Angebot

Es bestehen viele Angebote von digitalen Services: Private Dienstleister geben elektronische Identitäten aus, es mangelt nicht an Software-Lösungen oder an Such-Algorithmen. Häufig haben wir es deshalb nicht mit einem fehlenden Angebot zu tun. Im Bereich der *Dateninfrastrukturen* hingegen ist das Angebot noch mangelhaft. Deshalb spielt das Kriterium digitales Angebot vor allem im Bereich der Dateninfrastrukturen eine grosse Rolle. Das Angebot muss benutzerfreundlich, zugänglich, über eine ausreichende Performance und einen ausreichenden Funktionsumfang verfügen.

B) Wahlfreiheit

Wenn es einen digitalen Service gibt, ist zu prüfen, ob die Wahlfreiheit gegeben ist. Abhängigkeiten zu Anbietern (Vendor Lock-in) verhindern häufig die Wahlfreiheit, da die Wechselkosten (switching costs) von einem System in ein anderes enorm hoch sind. Wo die Wahlfreiheit verletzt wird, sollte der Staat mindestens prüfen, ob mit vertretbarem Aufwand und technologischer Kapazität ein Service Public Angebot aufgebaut werden kann oder die Unterstützung von Alternativen möglich ist, um Wahlfreiheit zu schaffen.

C) Vertrauenswürdigkeit

Vertrauenswürdig sind digitale Services, wenn Sicherheit, Transparenz und Nachvollziehbarkeit gewährleistet sind. Der Staat geniesst in der Schweiz ein hohes Vertrauen, sodass im Falle einer Abwägung dieses Kriterium ausschlaggebend sein kann, ob der Staat seine Tätigkeit für einen digitalen Service erweitern soll oder nicht. Wenn die Bürger*innen einem privaten Anbieter vertrauen, ist aus ordnungspolitischer Sicht kein Eingreifen notwendig.

1.2 Relevanz und Aufbau der Studie

In der politischen Debatte um die Auswirkungen der Digitalisierung ist Kritik am Status quo mittlerweile weit verbreitet. Die Relevanz der vorliegenden Fragestellung ergibt sich durch zahlreiche zivilgesellschaftliche als auch staatliche Initiativen, primär aus dem nationalen oder europäischen Umfeld. Antworten sind an unterschiedlichen Orten zu finden:

- **Zivilgesellschaftliche Organisationen,** die sich mit ökonomischen, gesellschaftlichen und politischen Auswirkungen der Digitalisierung befassen und sich einer Advocacy-Agenda verschrieben haben (z.B. Open Knowledge Foundation, European Digital Rights EDRi, AlgorithmWatch, Digitale Gesellschaft Schweiz / Deutschland);
- **Internationale Regierungsorganisationen,** die entweder selbständig (OECD, EU, UNO) oder im Verbund (Digital Public Goods Alliance) eine regierungsberatende Agenda verfolgen;
- **Nationale Multistakeholder-Organisationen** wie die Swiss Data Alliance (SDA), die Swiss Digital Initiative, digitalswitzerland oder das Swiss IGF (Internet Governance Forum);
- **Wissenschaftliche Akademien,** die sich mit technologischen Entwicklungen befassen (z.B. die deutsche Akademie der Technikwissenschaften, acatech);
- ***Open Source* Förderorganisationen** wie CH Open (Schweiz) oder die Open Source Business Alliance (OSB) Alliance (Deutschland), die sich als Teil der weltweiten Open Source Bewegung verstehen und sich für die Verbreitung und Nutzung von Open Source Software einsetzen.

In den Publikationen und Aktivitäten gibt es zurzeit keinen Konsens darüber, welche Rolle der Staat angesichts der fortschreitenden Digitalisierung generell einnehmen soll. Es handelt sich auch nicht um fundamentale, digitalisierungskritische Interessenvertreter, die das Rad der Geschichte zurückdrehen möchten. Dennoch ist all deren Überlegungen die Sorge gemein, dass die bisher kaum regulierte und/oder durch staatliche Abwesenheit ungehindert fortschreitende technologische und wirtschaftliche Dominanz der *Hyperscaler* Abhängigkeiten auf der individuellen (als User dieser Services) als auch auf staatlicher Ebene (etwa im Bereich der elektronischen Identitäten, in der Gesundheitsversorgung, in der Schulinformatik oder im Mediensystem) geschaffen hat, welche als unbefriedigend wahrgenommen werden (vgl. dazu Abschnitt 2.2). Möglichst neutral formuliert, könnte aus der Betrachtung der ökonomischen Theorie von einem Marktversagen gesprochen werden, indem die Art und Weise, wie die IT-Services erbracht werden, Abhängigkeiten schaffen (Lock-in-Effekte, vgl. Abschnitt 2.5). Die oben genannten Organisationen befassen sich in der Regel aber nicht mit einer Analyse digitaler Märkte aus politökonomischer Perspektive. Vielmehr stellen sie die Abhängigkeiten fest und beklagen implizit ein Defizit des Public Value-Denkens. In der Ökonomie, wie auch im Recht, ist ebenfalls unklar, ob es sich tatsächlich um ein Marktversagen handelt. Skeptisch äussert sich etwa Richard Sturn: Digitale Monopole würden sich kaum durch Regulierungen, wettbewerbspolitische Eingriffe oder Besteuerung von Monopolrenten beseitigen lassen (Sturn, 2021, S. 19).

Welche Rolle soll der Staat im digitalen Raum spielen? Umfassende Konzepte entwickeln sich erst – aber die gemeinsame Klammer, so die Perspektive des vorliegenden Berichts, bilden die Überlegungen um die *digitale Souveränität* oder *digitale Selbstbestimmung*.

> «Was uns heute fehlt, ist eine Behandlung der übergreifenden Fragen der Beherrschung der Digitalisierung: Die Rolle des Staates im digitalen Raum, sein Auftrag bei der digitalen

> Daseinsvorsorge[6], die Grundfragen eines neuen Digitalrechts – all das wird bislang nicht ausreichend politisch sichtbar und prominent bearbeitet. Gerade hier aber haben Staat und Politik einen Auftrag zu erfüllen, der einen langen Atem erfordert, kluge und gut ausgebildete Experten, intensiven gesellschaftlichen Dialog» (Schallbruch, 2022).

Die Digitalisierung verlangt nach einer neuen Bewertung des Begriffs Service Public, denn die sich in den vergangenen 20 Jahren herausgebildete Internet-Ökonomie hat zu neuen Defiziten (Marktversagen) geführt (Kapitel 2). Im Kapitel 3 werden entlang einem Technologie-Schichtenmodell mit acht Ebenen die Herausforderungen eines zukünftigen Digitalen Service Public aufgezeigt. Kapitel 4 diskutiert das Konzept *Government as a Plattform*. In Kapitel 5 werden schliesslich die Ergebnisse zusammengefasst und Empfehlungen für einen Digitalen Service Public aufgestellt. Ein Fazit mit Ausblick erweitert zum Schluss relevante, aber nicht untersuchte Fragen zur Thematik.

1.3 Service Public im geltenden Recht

Der Begriff «Service Public» wird in einem bundesrätlichen Bericht aus dem Jahr 2004 mit «Grundversorgung in der Infrastruktur» gleichgesetzt[7]. Die Grundversorgung ist auf nationaler Ebene teilweise in der Verfassung sowie im Radio-und-TV-Gesetz, im Fernmeldegesetz, im Postgesetz, im Stromversorgungsgesetz und vereinzelt auch auf Verordnungsstufe geregelt. In der Verfassung findet sich der Begriff «Grundversorgung» in Art. 43a BV (Grundsätze für die Zuweisung und Erfüllung staatlicher Aufgaben), in Art. 92 BV (Post- und Fernmeldewesen) sowie in Art. 117a BV (Medizinische Grundversorgung). Sowohl Art. 43a BV als auch Art. 117a BV wurden erst nach dem oben erwähnten Bericht des Bundesrates aus dem Jahr 2004 in die Verfassung eingefügt.

In Art. 43a Abs. 4 BV ist festgehalten, dass Leistungen der Grundversorgung allen Personen in vergleichbarer Weise offenstehen müssen. Gemäss Biaggini (Reiners, 2021) bleibt die rechtliche und praktische Bedeutung dieses Absatzes diffus, «dies jedenfalls, solange nicht klar ist, was von Bundeverfassungsrechts wegen zur Grundversorgung gehört» (Biaggini, 2017). Der am 18. Mai 2014 in Kraft getretenen Art. 117a BV (Medizinische Grundversorgung) wird bei Biaggini nicht erwähnt. Diese Bestimmung begründet keine neuen Kompetenzen des Bundes und der Kantone und führt auch nicht zu einer neuen Kompetenzaufteilung[8]. Klar ist nur, dass die Grundversorgung mit Post- und Fernmeldediensten in allen Landesgegenden von der Verfassung verlangt wird (Art. 92 Abs. 2 BV).

Eine Motion aus dem Jahr 2005 mit der Forderung nach einer Verfassungsbestimmung über die Grundversorgung ist 10 Jahre nach der Einreichung (und zunächst Annahme durch beide Kammern) im September 2015 abgeschrieben worden[9]. Gleichzeitig wurden auch die Arbeiten an einer Verfassungsbestimmung, die der Bundesrat gegen seinen Willen dem Parlament vorgelegt hat, durch den Nationalrat gestoppt (SDA, 2015)[10].

[6] Der Begriff der Daseinsvorsorge entspricht in der Schweiz dem Begriff Service Public.

[7] Bericht des Bundesrates «Grundversorgung in der Infrastruktur (Service Public)» vom 23. Juni 2004 (BBl 2004 4569).

[8] BSK BV-Gächer/Renold-Burch, Art. 117a BV N 25.

[9] Motion der Kommission für Verkehr und Fernmeldewesen (05.3232): Verfassungsbestimmung über die Grundversorgung.

[10] SDA-Meldung vom 8. September 2015: Nationalrat versenkt neuen Grundversorgungsartikel.

Auf gesetzlicher Ebene ist die Grundversorgung im Bundesgesetz über Radio und Fernsehen, im Fernmeldegesetz sowie im Postgesetz und im Stromversorgungsgesetz geregelt, wobei nicht immer der Begriff «Grundversorgung» verwendet wird. Teilweise findet sich die Definition der Grundversorgung auch erst auf Verordnungsstufe, dies gilt insbesondere für den Bereich des öffentlichen Verkehrs.

Das aktuell geltende RTVG sieht Grundversorgungsanbieter vor, die zur Erfüllung des verfassungsrechtlichen Grundversorgungsauftrags verpflichtet sind, entsprechend finanziell unterstützt bzw. verbreitungstechnisch privilegiert werden und grundsätzlich das Vielfaltsgebot zu beachten haben (Piolino, 2021, S. 141). Diesen Grundversorgungsanbietern stehen Veranstalter ohne Leistungsauftrag gegenüber, die lediglich einer Meldepflicht unterliegen (vgl. Art. 3 lit. a RTVG) und Tendenzfreiheit geniessen. Indem das RTVG somit auch meldepflichtige Veranstalter zulässt, die nicht zur Erfüllung des verfassungsrechtlichen Grundversorgungsauftrags verpflichtet sind, wird ein sog. duales System ohne Grundversorgungsmonopol etabliert (Piolino, 2021, S. 141).

Das Fernmeldegesetz soll u.a. eine zuverlässige und erschwingliche Grundversorgung mit Fernmeldediensten für alle Bevölkerungskreise in allen Landesteilen gewährleisten (Art. 1 Abs. 2 lit. a FMG). Im Abschnitt «Grundversorgungskonzession» ist zunächst die Vergabe der Grundversorgungskonzession(en) durch die Eidgenössische Kommunikationskommission (ComCom) geregelt. Die weiteren Bestimmungen regeln u.a. die Konzessionsvoraussetzungen, den Umfang der Grundversorgung, Qualität und Preise und die finanzielle Abgeltung.

Im Postgesetz ist die Grundversorgung in Art. 13 ff. geregelt. Die Post stellt die Beförderung von Briefen, Paketen, Zeitungen und Zeitschriften sicher (Art. 14 Abs. 1 PG). Sie stellt diese Postsendungen an mindestens fünf Wochentagen zu (Art. 14 Abs. 3 PG) und stellt landesweit ein flächendeckendes Netz von Zugangspunkten sicher (Art. 14 Abs. 5 PG). In Art. 15 ff. PG sind die Qualität, die Preise und weitere Rechte und Pflichten der Post geregelt.

Das Stromversorgungsgesetz enthält einen aus zwei Artikeln (Art. 5 und 6 StromVG) bestehenden Abschnitt mit dem Titel «Gewährleistung der Grundversorgung». Art. 5 StromVG regelt die Netzgebiete und Anschlussgarantie. Gemäss Art. 5 Abs. 2 StromVG sind Netzbetreiber verpflichtet, in ihrem Netzgebiet alle Endverbraucher innerhalb der Bauzone und ganzjährig bewohnte Liegenschaften und Siedlungen ausserhalb der Bauzone sowie alle Elektrizitätserzeuger an das Elektrizitätsnetz anzuschliessen. In Art. 6 StromVG sind die Lieferpflicht und Tarifgestaltung für feste Endverbraucher geregelt. Gemäss Art. 6 Abs. 1 StromVG treffen die Betreiber der Verteilnetze die erforderlichen Massnahmen, damit sie in ihrem Netzgebiet den Endverbrauchern jederzeit die gewünschte Menge an Elektrizität mit der erforderlichen Qualität und zu angemessenen Tarifen liefern können.

Schliesslich können auch das Eisenbahngesetz und das Personenbeförderungsgesetz als Grundversorgungsgesetze betrachtet werden, wobei der Begriff «Grundversorgung» in diesen nicht vorkommt. Der Umfang der Grundversorgung ist in der Verordnung über die Abgeltung des regionalen Personenverkehrs geregelt[11]. Im Bereich des öffentlichen Verkehrs im Bereich des Strassenverkehrs wird der Grundversorgungsbegriff ebenfalls kaum verwendet[12].

[11] BR-Bericht, S. 4593.

[12] BR-Bericht, S. 4595.

1.4 Europäischer Referenzrahmen und technologische Abhängigkeiten

Die bereits im Vorfeld durchgeführten Workshops mit Expert*innen aus der Bundesverwaltung sowie aus Grundversorgungsunternehmen stossen in der Diskussion über Digitalisierung immer wieder an konzeptionelle Grenzen. Die lineare Weiterführung der Diskussion: «Wo hat der Staat neu einen Grundversorgungsauftrag?» hat in den vom BAKOM organisierten Diskussionen sich als wenig fruchtbare Diskussionsbasis gezeigt (BAKOM, 2021a, 2021c). Die Herausforderung der digitalen Transformation würde eine Digitalpolitik erfordern, bevor schliesslich die Frage nach einer Ausweitung des Grundversorgungsauftrages gestellt wird. Um Orientierung zu schaffen, soll kurz skizziert werden, wie sich eine «Digitalpolitik» innerhalb der EU entwickelt hat. Dabei werden wichtige Bestandteile frei gelegt (Reiners, 2021).

2015 – 2017: Digitaler Binnenmarkt

In dieser Phase propagierte die EU-Kommission einen digitalen Binnenmarkt. Legislativ erfolgte die Datenschutzgrundverordnung, Förderung des E-Commerce, Aufbau einer europäischen Datenwirtschaft, ein Plan für die digitale Bildung, Breitbandversorgung, 5G sowie Cybersicherheit.

2017 – 2020: Aussen- und sicherheitspolitische Dimension

Die aussen- und sicherheitspolitische Dimension der Digitalisierung wird dominant aufgrund des Datenverkehrs mit Drittstaaten in Handelsabkommen, Fragen der Cybersicherheit und der Spionageabwehr; die Digitalisierung wird vermehrt als Sicherheitsbedrohung wahrgenommen und in die Gemeinsame Aussen- und Sicherheitspolitik (GASP) integriert.

Seit 2020: Digitale Dekade, Green Deal und Covid-19 Krise

Mit der neuen Legislatur (2019-2024) verankert der EU-Rat die Digitalpolitik definitiv in die neue strategische Agenda; die Staats- und Regierungschefs fordern eine «digitale Souveränität»; die EU soll «für das digitale Zeitalter gerüstet sein», heisst eines von sechs übergeordneten Zielen. Europa soll in kritischen Technologiebereichen souverän werden. Ausserdem knüpft der Green Deal ebenfalls an ein digital souveränes Europa an, indem das Potenzial der Verfügbarkeit von (Umwelt-)Daten betont wird.

Die normative Grundlage für eine Serie von neuen digitalpolitischen Initiativen besteht aus drei Bausteinen:

- Digitale Kompetenzen, Schutz von Cyberbedrohungen, KI, ultraschnelle Breitbandverbindungen, Ausbau von Hochleistungsrechenkapazitäten als «Technologie im Dienst des Menschen»;
- Eine faire und wettbewerbsfähige Wirtschaft durch Regulierung von Online-Plattformen, und den Wettbewerb im Binnenmarkt, Verbesserung des Zugangs zu Daten;
- «Eine offene, demokratische und nachhaltige Gesellschaft» durch die Verbindung von Initiativen zur Verwirklichung der Klimaneutralität, Nutzung von Gesundheitsdaten, Datenschutz und Bekämpfung von Desinformation.

Die Überlegungen der EU-Kommission können auch auf die Schweiz übertragen werden. Anstatt ausschliesslich das Marktversagen zur Legitimation für die Erweiterung der Grundversorgung heranzuziehen, könnte vielmehr nach den Zielvorstellungen der Gesellschaft gefragt werden. So kann man den Überlegungen der Open Future-Gründer Paul Keller und Alek Tarkowski (Keller & Tarkowski, 2021) und des Ökonomen und Juristen Andrea Renda (Renda, 2020) folgen. In beiden grundlegenden Publikationen wird die Vorstellung eines «digital ecoystem» (Renda, 2020) oder eines «digital space» innerhalb der Europäischen Union entworfen. Dabei wird versucht, die zahlreichen digitalpolitischen Initiativen von Kommission und Parlament in der laufenden Dekade als umfassendes politisches Konzept jenseits klassischer Politikfelder zu denken. In eine ähnliche Richtung geht auch der Bericht «European Public Sphere» (Kagermann et al., 2021) von acatech, der deutschen Nationalen Akademie der Wissenschaft und Technik. Ob sich der Begriff digitales Ökosystem, digitaler Raum oder digitale Sphäre durchsetzen wird, ist unbedeutend, aber als Referenz für die Frage, worin die Konsequenzen der Digitalisierung für die staatliche Aufgabenerfüllung (Daseinsvorsorge, Grundversorgung) bestehen, sind die Visionen sehr hilfreich.

Die besondere Herausforderung der Digitalisierung aus der Perspektive einer national verfassten Gesellschaft ist, dass die Wirtschaft sehr umfangreiche und häufig (auf den ersten Blick) kostenlose Dienstleistungen erbringt, wobei es sich bei den Anbietern meist um internationale Grosskonzerne handelt. Diese Entwicklung ist weit fortgeschritten und hat sich ohne staatliche Beteiligung oder gar Regulierung durchgesetzt. An und für sich hoheitliche Aufgaben wie den Bürger*innen eine Identität auszustellen, wären eigentlich eine Aufgabe des Staates, doch die Digitalisierung hat alternative Identitätslösungen erschaffen, die etwa beim Abschluss eines Kaufs benötigt werden (Rötzer, 2020). Auch die sozialen Plattformen benötigen zwar eine Identität der Nutzenden, allerdings braucht es keine staatliche Anerkennung dieser.

Die Vorstellung der EU, diejenigen Bereiche souverän zu gestalten, welche durch die privatwirtschaftlich vorangetriebene Digitalisierung sich stark verändert haben, benennt die «Komponenten» der digitalen Transformation. Neben der Kontrolle des Cyberraumes gehören die technischen digitalen Systeme (Hardware, Software, Infrastruktur, Standards und Protokolle) sowie Datensammlung, der Datenfluss und der -Zugriff dazu. Weiter reicht die Frage nach digitaler Souveränität in wirtschaftliche und gesellschaftliche Bereiche hinein, wenn die Digitalisierung Wettbewerbsbedingungen verändert.

1.5 Technologie-Schichtenmodell

Da es bisher keine systematische Betrachtung zur Rolle des Staates in der Digitalisierung gibt, hat die Deutsche Akademie der Technikwissenschaften ein Modell entwickelt, das die Frage nach einer europäischen digitalen Souveränität differenziert für einzelne technologische Ebenen stellt (Kagermann et al., 2021). Unter der Digitalen Souveränität wird dabei die Fähigkeit von Individuen, Unternehmen und Politik verstanden, frei zu entscheiden, wie und nach welchen Prioritäten die digitale Transformation gestaltet werden soll. Technologie und Daten stellen gemäss dem Verständnis der

Autor*innen Hebel dar, mit denen digitale Souveränität erreicht wird. Weiter braucht es auch Massnahmen im Bereich der digitalen Kompetenzen von Unternehmen, öffentlichen Einrichtungen und Fachkräften, sowie geeignete Regulation des digitalen Binnenmarktes zur «industriepolitischen Begleitung» (Kagermann et al., 2021, 8). Mit einem Fokus auf den Technologie- und Datenhebel schlagen Kagermann et al. ein Technologie-Schichtenmodell mit acht Ebenen vor, entlang welchen Technologien nach dem Grad der Digitalen Souveränität bewertet werden können (siehe nachfolgend Tabelle 1). Bei den Ebenen handelt es sich dabei um die «relevantesten, machbarsten und aktuell mit dem grössten politischen Handlungsbedarf verbundenen Technologiefelder» (Kagermann et al., 2021).

Die von Kagermann et al. vorgeschlagene Aufteilung in acht Ebenen eignet sich auch, um Entwicklungen in der Schweiz einzuordnen – selbst wenn Politik und Gesellschaft zum Schluss kommen sollten, dass die Souveränität entweder nicht, nur eingeschränkt oder im internationalen (=europäischen) Verbund wünschbar wäre. Das Modell will die Stärken und Schwächen, sowie die Verwundbarkeiten je Ebene analysieren, weil dies die Voraussetzung ist, zu regulieren oder mit Industriepolitik die Abhängigkeit von den Hyperscalern (z.B. IBM, Amazon, Microsoft und Google) zu reduzieren. Der Zweck von digitaler Souveränität wird dabei nicht in einem digitalen Protektionismus gesehen, sondern in der Ermöglichung einer Gestaltungs- und Wahlfreiheit für oder gegen eine Technologie. Digitale Souveränität baut demnach auf einer Vielzahl von Angeboten auf, wobei globale Technologieunternehmen zu europäischen Bedingungen eingebunden werden sollen – insbesondere im Hinblick auf Cybersicherheit, Datenschutz und Persönlichkeitsrechte (Kagermann et al., 2021, S. 9).

Tabelle 1 Ebenen des Technologie-Schichtenmodells nach Kagermann et al. (2021)

	Ebene	Bestandteile / Fokusbereich
7	Europäisches Rechts- und Wertesystem	Cybersecurity, Kryptografie, E-Identity, EU-Zertifizierung (Verbraucherschutz) und Standards
6	Softwaretechnologien	App-Entwicklungen, Office, ERP, KI, Middleware, Robotik-Software, Blockchain, Algorithmen, EU- Open Source, VR/AR, QC
5	Europäische Datenräume	Zum Beispiel für Mobilität, Health, Public Sector, digitaler öffentlicher Raum
4	Platform-as-a-Service (PaaS)	Anwendungs- und Entwicklungsökosysteme B2B und B2C (Abstraction Layer, Container Technology) QC, KI, IoT
3	Infrastructure-as-a-Service (IaaS)	Virtuelle, verteilte Cloud-Ökosysteme, Edge-Technologie, QC, KI-HPC-Center
2	Kommunikationsinfrastruktur	Breitbandinfrastruktur, Mobilfunknetze (Open RAN), Galileo-Navigation
1	Komponenten	Mikrochips, Sensoren, Aktuatoren, Fertigungs- und Basistechnologien, 3D-Druck, QC, KI
0	Rohmaterialien und Vorprodukte	Seltene Erden

In diesem Bericht werden wir in Kapitel 3 auf die Ebenen 2 bis 7 näher eingehen.

2 Neue Herausforderungen für den Staat durch Digitalisierung

Kapitel 2 thematisiert die technologischen und ökonomischen Herausforderungen im Zuge der Digitalisierung und gibt eine konkrete Einschätzung von den Herausforderungen, die im Auftrag als «völlig neue Service Public-Bedürfnisse (das heisst Infrastrukturen oder Dienstleistungen)» angesprochen werden.

Im digitalen Zeitalter verschieben sich die Bedürfnisse der Individuen und des Kollektivs. Schnelles Internet und Zugang auf digitale Services entsprechen dem Gebot nach sozialer Teilhabe ebenso sehr wie Strom, Wasser oder Energie. Schulz beschreibt für Deutschland die «digitale Daseinsvorsorge» als «Auftrag und die Pflicht des Staates, eine angemessene, d. h. den jeweiligen zeitlichen und örtlichen, wirtschaftlichen und technischen Gegebenheiten angepasste Grundversorgung möglich zu machen, soweit diese nicht vom Markt oder gemeinnützigen Akteuren angeboten wird (Subsidiaritätsprinzip)» (Schulz, 2020). In der Schweiz ist die Daseinsvorsorge, bzw. der Service Public auch nicht definiert, sondern Ergebnis eines politischen und gesellschaftlichen Aushandlungsprozesses. Auch diese Studie wird nur Anregungen geben können, welche Defizite einer zu bestimmenden Grundversorgung bestehen bzw. ob in den bestehenden (privaten) Angeboten Defizite bezügliche der Wahlfreiheit oder Vertrauenswürdigkeit bestehen.[13] Eine Referenz für solche Beurteilungen bildet aber die internationale und europäische Debatte über Daseinsvorsorge, Universaldienst oder «universal services»; davon abgeleitet werden die Entwicklungen auf die Schweiz übertragen. Welche neuen Aufgaben im digitalen Zeitalter zur öffentlichen Daseinsvorsorge gehören, also vom Staat garantiert werden sollen, wenn der Markt nicht für entsprechende Angebote sorgt, ist nicht abschliessend geklärt. Allerdings geht man davon aus, dass ein Digitaler Service Public mehr ist als die Versorgung mit Breitband.

2.1 Datenräume/Daten-Infrastrukturen

Was unter einem *Datenraum* zu verstehen ist, soll kurz am Beispiel von multimodalen Mobilitätsdienstleistungen erläutert werden (Ecoplan, 2019), sowie anhand des Berichts von swisstopo zum «Verkehrsnetz CH»[14]. Im Bereich des Verkehrs sind die Überlegungen zu einem Datenraum als Service Public konzeptionell, aber auch von der gesetzlichen Anpassung her, weit fortgeschritten. Das Gut «Daten» weist gemäss der Studie von ecoplan die typischen ökonomischen Eigenschaften eines Infrastrukturgutes auf (Ecoplan, 2019). Die Auffassung, dass Daten als Infrastruktur bezeichnet werden können, findet sich auch in der Open Government Data (OGD) Strategie des Bundesrats 2019-2023[15]. Damit aber Daten zu einem Infrastrukturgut werden, müssen sie möglichst umfassend sein, was nur dann gelingt, wenn unterschiedliche Datenlieferanten mit ihren unterschiedlichen Verwertungsinteressen ihre Daten teilen (zur Problematik von Datensilos im öffentlichen Sektor siehe

[13] Mehr zu den Defiziten im Framework (Abschnitt 5.3)

[14] Verkehrsnetz Schweiz- Kurzbericht, Bericht an den Bundesrat zu den wesentlichen Fragen für die Realisierung (31.12.2021) (www.swisstopo.admin.ch/de/swisstopo/verkehrsnetz-schweiz.html#288_1584718351847).

[15] «Daten als Infrastruktur zu bezeichnen, bedeutet, sie als Teil der Basisausstattung für das gute Funktionieren von Gesellschaft, Politik und Wirtschaft zu verstehen. Als nicht rivalisierendes Gut (Konsum durch eine Person beeinträchtigt nicht den Konsum durch eine andere Person) werden Daten als Input für unterschiedlichste Zwecke genutzt, sie können also gemeinsames Mittel für viele Zwecke sein» (https://www.fedlex.admin.ch/eli/fga/2019/125/de)

auch 2.3). Eine solches «Data Sharing» widerspricht allerdings meist dem jeweiligen privaten Geschäftsinteresse, weshalb ein soziales Dilemma bzw. ein Marktversagen auftreten kann. Der Gesellschaft entgehen so zusätzliche Dienstleistungen; allfällige Innovationen werden gar verhindert.

Relevant für die Vorstellung der Weiterentwicklung des Service Public zu einem Digitalen Service Public sind die Überlegungen, wonach Daten aus einem zusammenhängenden Bereich durch eine Integration zur Dateninfrastruktur werden können und damit einen zusätzlichen Wert erhalten, der über den Wert des Datenproduzenten hinaus geht. Bezugnehmend auf die EU-Datenstrategie[16] vertritt in der Schweiz besonders die Swiss Data Alliance (SDA) das Konzept der «*Dateninfrastrukturen*» in ihrem Whitepaper (Swiss Data Alliance, 2021)[17]. Öffentlichen Daten sollen in einer «EU-weiten Dateninfrastruktur» grenzüberschreitend in einem Europäischen Datenraum zusammengefasst werden (Swiss Data Alliance, 2021).Die konkrete Umsetzung dieser Datenräume ist – mit Ausnahme des Fallbeispiels zur Mobilität – nicht Bestandteil des vorliegenden Berichts.[18] Zur Zeit sind auf nationaler und auf EU-Ebene verschiedene Datenräume in Diskussion, u.a. Umwelt, Energie, Mobilität, Finanzen, öffentliche Verwaltung, Forschung, Wissenschaft und Innovation und Gesundheit. Zwei dieser «Datenräume» sollen im Hinblick auf die Frage nach dem Service Public näher beschrieben werden: Mobilität und Gesundheit (Abschnitte 3.3.1. und 3.3.2).[19]

2.2 Privatisierung des digitalen Raums durch dominierende Plattform-Anbieter

Digitale Plattformen, insbesondere die «Big Five» genannten Alphabet (Google), Meta (Facebook), Amazon, Apple und Microsoft, bilden ein mächtiges gewinnorientiertes Ökosystem, das aus unserem heutigen Alltag praktisch nicht mehr wegzudenken ist. Durch ihre Omnipräsenz dominieren diese Plattformen die Infrastruktur für die Bereitstellung und Verteilung von Online-Services wie Informationen, sowie Möglichkeiten zur sozialen und privaten Kommunikation (van Dijck, 2021). Der Einfluss der Big Five ist dabei sowohl auf Infrastrukturebene (z.B. Cloud-Lösungen, Datenzentren, Unterseekabel), auf intermediärer Ebene (z.B. mit sozialen Netzwerken, Login- und Identifikationsservices, Such- und Navigationssystemen etc.) sowie auf sektoraler Ebene ersichtlich (z.B. Bildungsapplikationen, Gesundheitsapplikationen, etc.), wobei zunehmend auch öffentliche Akteure für zentrale ökonomische und demokratische Funktionen von diesem globalen System abhängig sind (van Dijck, 2021). Ihre enorme Macht erhalten die Plattformen gemäss van Dijck auf zwei Wegen: Einerseits durch die die Zusammenführung von Technologieunternehmen, die sowohl infrastrukturelle als auch sektorale Plattformen betreiben, und andererseits durch die Schaffung und Gestaltung der der Plattform-Ökonomie zugrunde liegenden Mechanismen – der Lenkung von Datenströmen, der Einbindung von Nutzern und deren Daten sowie der Etablierung von Auswahlkriterien und

[16] Europäische Kommission: Europäische Datenstrategie (ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de)

[17] https://drive.google.com/file/d/1FhUEQfRF9mI9p0Fhbxz6FVKYqOSfu-Hc/view?usp=sharing

[18] Zur konzeptionellen Umsetzung von Dateninfrastrukturen mithilfe von Software-Architekturen vgl Otto und Burmann (2021).

[19] Vgl. zu den Datenräumen ausführlich Bericht «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung» (UVEK und EDA (2022)) UVEK und EDA (2022)

algorithmischen Lock-ins, welche zu einer Pfadabhängigkeit führen (van Dijck, 2021). Für die Öffentlichkeit besteht gegenüber all jenen Mechanismen grosse Intransparenz.

Wiederkehrende Diskussionen auf politischer und gesellschaftlicher Ebene illustrieren die wachsende Besorgnis angesichts der Übermacht dieser Plattformen. Der Fokus liegt dabei meist auf deren Einfluss auf die Wettbewerbsfreiheit, sowie der Meinungsfreiheit und -vielfalt. Auf europäischer Ebene hat die EU-Kommission Ende 2020 zwei Vorschläge veröffentlicht: den Digital Markets Act (DMA) und den Digital Services Act (DSA). Während der DMA einen Fokus auf Wettbewerbspolitik legt – ein faires Verhalten der sogenannte «Gatekeeper»-Plattformen soll sichergestellt werden (Europäische Kommission, 2020a) – skizziert der DSA neue Regeln und Verantwortlichkeiten für User, Plattformen und öffentliche Akteure «gemäss europäischen Werten», wobei der Fokus auf den Bürger*innen und dem gesellschaftlichen und demokratischen Diskurs liegt (Europäische Kommission, 2020b).

Die Plattform-Diskussion erschöpft sich allerdings nicht in Fragen der Markt- und Meinungsmacht, da der Einfluss von Plattformen wie Google & Co. viel weitreichender ist (Busch, 2021; van Dijck, 2021). Busch nennt drei Mechanismen, wie Plattformen, deren digitale Infrastruktur und Daseinsvorsorge (definiert als die durch das Gemeinwesen sicherzustellende Versorgung von Gütern und Dienstleistungen) zusammenwirken (Busch, 2021). Einerseits stellt sich durch die digitale Transformation zunehmend die Frage nach einer Daseinsvorsorge im digitalen Raum. Andererseits kann in traditionellen Bereichen der Daseinsvorsorge eine zunehmende Digitalisierung beobachtet werden, bei der Plattformen immer wichtiger werden. Und schliesslich stellt sich die Frage, ob die Plattformen der Big Five durch ihre Durchdringung des gesellschaftlichen Lebens nicht inzwischen selbst als Grundversorgung gelten könnten oder sollten.

Hinzu kommt, dass es in Bereichen wie dem Gesundheits- oder dem Bildungswesen wahrscheinlich ist, dass private Plattformanbieter auf kurze Frist schneller stabilere Infrastrukturen zur Digitalisierung anbieten können, was Schallbruch am Beispiel Grossbritanniens illustriert: Um von den Rechenkapazitäten und Algorithmen Googles zu profitieren, habe der National Health Service (NHS) rund 1.6 Millionen Patientendaten an die Plattform übertragen (Schallbruch, 2022). Es besteht demnach Grund zur Annahme, dass die *Plattformisierung* somit auch zunehmend Einfluss auf das Gemeinwohl («common good») nimmt, weshalb digitale Plattformen heute als Infrastrukturen der digitalen Daseinsvorsorge bezeichnet werden können (Busch, 2021). Es ist diese Unverzichtbarkeit der für die Gesellschaft unterdessen wesentlichen Dienstleistungen, die den Anspruch des Staates begründet, dem Dienstleister gemeinwohlorientierte Pflichten aufzuoktroyieren (Busch, 2021).

2.3 Datensilos

Unsere Gesellschaft produziert riesige Mengen an Daten. Bereits 2018 wurde die weltweit produzierte Menge an Daten auf ca. 33 Zettabyte (1 Zettabyte ist gleich eine Trillion Gigabytes) geschätzt, für 2025 wird eine Zunahme von 530 Prozent auf 175 Zettabyte prognostiziert (Europäische Kommission, 2022). In der EU-Datenstrategie wird der Wert der Daten für das Jahr 2025 auf 829 Milliarden Euro geschätzt (Europäische Kommission, 2022). Daten haben aber nicht nur einen volkswirtschaftlichen, sondern einen hohen gesellschaftlichen Wert. Denn Daten können als Grundlage für wichtige politische Entscheidungen und Strategien in praktisch allen Sektoren dienen, darunter viele im Bereich des Service

Public – beispielsweise Gesundheit, Bildung oder Mobilität. Ganz allgemein können Daten auch dazu verwendet werden, die Dienstleistungen der öffentlichen Verwaltung für ihre Bürger*innen zu verbessern. Die öffentliche Verwaltung, die selbst eine erhebliche Menge an Daten produziert, könnte zur Realisierung dieses Potentials einen grossen Beitrag leisten. In vielen Fällen wird dies aber durch das Fortbestehen sogenannter Datensilos verhindert.

Mit Datensilos ist die verstreute und wenig verknüpfte Datenhaltung der öffentlichen Verwaltung gemeint. Eine rechtliche und technische Trennung der Daten verhindert, dass diese umfassend genutzt werden können (Schallbruch, 2018). Damit die Daten von anderen öffentlichen Institutionen, der Forschung und privaten Akteurinnen wie KMUs oder Start-ups sinnvoll genutzt und Public Value generiert werden kann, müssen die Daten aus verschiedenen öffentlichen Institutionen miteinander kombinier- und auswertbar sein, und es muss Klarheit über den rechtlichen Rahmen für die Datennutzung bestehen (Kommune21, 2021).

Stand aktuell liegt vor vielen Verwaltungen noch ein relativer langer Weg, wenn es darum geht, Silos niederzureissen und Kooperationen zu intensivieren. An vielen Stellen ist dazu vermutlich ein Paradigma-Wechsel nötig: Solange sich bundesnahe Unternehmen gegenseitig konkurrenzieren, werden Datensilos bestehen bleiben. Als grundsätzliches Gegenmodell zu Silos präsentiert sich das Konzept der vertrauenswürdigen Datenräume, basierend auf den Grundprinzipien von Transparenz, Kontrolle, Fairness, Verantwortlichkeit, Effizienz und Nachhaltigkeit. Dass das Zusammenführen von Daten in der Praxis eine grosse Herausforderung ist, zeigt das Projekt des elektronischen Patientendossiers, welches eine erste Form der Implementation eines vertrauenswürdigen Datenraumes im Bereich der Gesundheitsdaten darstellen würde (vgl. auch Abschnitt 3.3.2).

2.4 Sicherheit und Privacy, Vertrauen in staatliche Lösungen

Die Digitalisierung kann zur Zusammenlegung von Daten führen. Das bedroht die Privatsphäre direkt, weil Daten in einem anderen Kontext genutzt werden als in dem, für den sie angelegt wurden. Es bedroht aber auch die Privatsphäre indirekt, weil anonymisierte Daten de-anonymisiert werden können (Hürlimann & Kettiger, 2021). Da zudem mehr Daten als je zuvor über Personen generiert werden und zugleich Cyberkriminalität ein nicht zu eliminierendes Phänomen darstellt, wächst die Bedrohung der Privatsphäre stetig an. Neben der Einschränkung der Privatsphäre, bedroht die Cyberkriminalität die Einwohner*innen und Unternehmen auch direkt, indem wertvolle nicht personenbezogene Daten und Eigentumsbeweise gestohlen oder IT-Systeme unbrauchbar gemacht werden.

Im physischen Raum haben der Staat und die ausführenden Organe auf allen staatlichen Ebenen die Aufgabe, Sicherheit, Leben und Eigentum ihrer Bürger zu schützen. Dafür bedient er sich der traditionellen, analogen Souveränität. Im digitalen Raum gibt es nur mehr sehr bedingt eine ortsgebundene Souveränität. Grenzen können nicht einfach geschlossen werden. Eine digitale Souveränität im Sinne einer Kontrolle der digitalen Medien unterliegt angesichts der erwünschten globalen Vernetzung klaren Einschränkungen. Trotzdem hat der Staat die Aufgabe, seine Einwohner*innen bestmöglichst zu schützen. Wie dies aber möglich ist, ohne einen Überwachungsstaat aufzubauen, ist derzeit unklar. Für die Bewältigung dieser Aufgaben sind zudem Kompetenzen im Bereich Digitalisierung notwendig (digital skills), die zukünftig weiter ausgebaut werden müssten.

Voraussichtlich wird der Staat das Engagement der Polizei und der Justiz in der Beobachtung des Internets, inklusive des Darknets, wesentlich ausbauen müssen. Darüber hinaus braucht es voraussichtlich zusätzliche Ressourcen, um die Einwohner*innen und Unternehmen bei der Selbsthilfe zu unterstützen. Es braucht vor allem Hilfe im Fall erfolgreicher Angriffe, die potenziell die Existenz zerstören können. Aber auch nach innen muss der Staat die Selbstkontrolle ausbauen. Denn auch ohne Cyberangriffe von aussen wächst durch die Integration der digitalen Ressourcen die Gefahr, dass die Privatsphäre der Einwohner*innen verletzt wird. Deshalb ist es gerade bei der fortschreitenden Weiterentwicklung des E-Government notwendig, den Datenschutz personell auszubauen.

2.5 Lock-in Effekte

Abhängigkeiten zu IT-Herstellern aufgrund von früheren Entscheidungen (Path Dependencies) sind in der Informatikbranche seit langem bekannt (Arthur, 1989). Bereits in den 90er-Jahren haben Firmen wie IBM mit ihren Mainframe-Systemen die Kunden durch Lock-in Effekt an sich gebunden (Greenstein, 1997). Später haben Hersteller von proprietärer Software ihre Nutzer abhängig gemacht, sodass sie kaum Alternativen wählen konnten (Xiaoguo Zhu & Zhizhong Zhou, 2011).

Heute schaffen die grossen Public Cloud-Anbieter wie Apple, Amazon, Alphabet (Google) und Microsoft neue Formen von «Vendor Lock-in», da sie bezüglich Funktionalität, Performance, Usability und Preis eine hohe Attraktivität geniessen und von Skaleneffekten profitieren. Die Gefahr ist gross, dass Nutzer dieser Cloud-Dienste in die Abhängigkeit der Anbieter geraten und nur mit hohen Wechselkosten (switching costs) den Anbieter wechseln können. Cloud-Services weisen meist proprietäre Datenformate auf, sowie eigene Applikationslogiken. Der Vendor Lock-in hat technische und organisatorische Ursachen (Mangel an Standardschnittstellen und offenen APIs). Betroffen von diesem Effekt sind individuelle Nutzer*innen ebenso wie Unternehmen und Behörden.

3 Technologie und Daten – Herausforderungen für den Digitalen Service Public

Strukturiert nach den Ebenen des Schichtenmodells[20] (Kagermann et al., 2021) werden im Kapitel 3 die bestehenden Lösungsansätze und Lücken bezüglich der Technologien und Daten erläutert und zukünftige Aufgaben des Staates im Hinblick auf die Sicherstellung einer digitalen Grundversorgung aufgezeigt. Am Ende des Kapitels wird das Schichtenmodell in Anlehnung an Kagermann et al. nochmals aufgenommen und in Bezug auf die Schweiz erweitert.

Das vorliegende Kapitel verwendet die technologischen Ebenen des acatec-Modells (vgl. Tabelle 1). Dabei werden die Ebenen 2, 3, 4, 5, 6 und 7 thematisiert. Ein digitaler Service Public wird in Zukunft beitragen, die digitale Souveränität zu gewährleisten. Dieser Begriff erfreut sich in jüngster Zeit wachsender Beliebtheit, ohne dass er bisher in der Schweiz näher konkretisiert worden wäre.[21]

Auf der technologischen Schicht 0 (Rohmaterialien und Vorprodukte) wird von den Autoren (Kagermann et al., 2021) keine Grundversorgung im Rahmen einer politischen Initiative angeregt. Sie schlagen den Einsatz der Circular Economy vor. Durch Wiederverwendbarkeit der Rohstoffe könnte die Abhängigkeit ein wenig reduziert werden. Für die Schweiz wird diese Schicht nicht analysiert.

Auf der technologischen Schicht 1 (Komponenten) hat die Europäische Kommission bereits einen «Chips Act» vorgelegt. Damit begeht sie einen industriepolitischen Weg, um der Versorgung des EU-Marktes aufgrund der Chip- und Halbleiterknappheit zu begegnen. 2021 kündigte die EU-Exekutive ihren Vorschlag für einen Chips Act an[22]. Aktivitäten der Schweiz werden für diese Schicht nicht untersucht.

3.1 Kommunikationsinfrastrukturen

Schichtenmodell Ebene 2

In der Kommunikationsbranche stellt die Vernetzungs-Infrastruktur eine zentrale Technologie-Grundlage dar, die mit den positiven Netz-Externalitäten nach den klassischen Regeln der Netzwerkökonomie funktioniert: Je mehr Personen in einem Netzwerk zusammengeschlossen sind, umso grösser ist deren individueller Nutzen (Knieps, 2007). Der staatliche Eingriff liegt in dieser Situation auf der Hand. Deshalb ist der Aufbau und Betrieb der Kommunikationsinfrastruktur detailliert über das Fernmeldegesetz (FMG) reguliert. Mit der fortschreitenden Digitalisierung treten laufend neue Dynamiken auf und machen deshalb die fortwährende Überarbeitung der Regulierung notwendig. So wurde 2020 das FMG insbesondere in Bezug auf die Netzneutralität (Poledna et al., 2017; Schlauri, 2010) revidiert. So ist nun eine Gleichbehandlung von Daten bei der Übertragung im Internet und der diskriminierungsfreie Zugang bei der Nutzung von Datennetzen gesetzlich geregelt.

[20] Die Ebenen 0 (Rohmaterialien) und 1 (Komponenten) werden gemäss der auftraggebenden Behörde nicht thematisiert.

[21] Mit dem gemeinsamen Bericht von UVEK und EDA zur «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung» (30.03.2022) wird allerdings zum ersten Mal für den Bereich der Datenräume eine ähnliche Stossrichtung aufgezeigt, vgl. https://www.newsd.admin.ch/newsd/message/attachments/70835.pdf.

[22] Pressemitteilung der Europäischen Kommission (8.02.2022) (Digitale Souveränität: Kommission schläft Chip-Gesetzvor, um Halbleiterknappheit anzugehen und Europas technologische Führungsrolle zu stärken), vgl ec.europa.eu/commission/presscorner/detail/de/ip_22_729

Der technologische Fortschritt und die wachsenden Bedürfnisse stellen heute erneut die Frage, wie der digitale Service Public in Zukunft aussehen soll. So steigt durch das Wachstum von Internet of Things (IoT)-Anwendungen die Nachfrage nach günstigen Funktechnologien, die Daten über weite Distanzen transferieren können. Diese so genannten «Long Range Wide Area Networks» (LoRaWAN) werden aktuell einerseits durch Anbieter wie die Swisscom aufgebaut[23]. Andererseits schaffen Crowd-Sourced Ansätze wie «The Things Network» die Möglichkeit für IoT-Anbieter, ihre Daten kostenlos zu übertragen (Blenn & Kuipers, 2017). Würden solche neuartigen Netzwerktechnologien staatlich gefördert und könnten dadurch Startups mit IoT-Lösungen wie BeeSmart[24] kostenlos ihre Geräte miteinander verbinden, würde dies die Durchdringung von IoT-Anwendungen unterstützen.

3.2 Infrastructure-as-a-Service/Platform-as-a-Service

Schichtenmodell Ebene 3 und 4

Gemäss der NIST-Definition von Cloud Computing aus dem Jahr 2011 (Mell & Grance, 2011) schafft «Infrastructure-as-a-Service» (IaaS) die Möglichkeit, Hardware-Ressourcen eines Servers (Festplattenspeicher, Arbeitsspeicher, Rechnerleistung etc.) zu virtualisieren und so bspw. über ein Web-Interface steuerbar zur Verfügung zu stellen. Dies ermöglicht eine sehr rasche und kostengünstige Möglichkeit, Server-Leistungen intensive zu nutzen, wenn sie tatsächlich benötigt werden und umgehend wieder zu reduzieren, wenn sie nicht mehr gebraucht werden. Einerseits fallen so die aufwändige Beschaffung und Wartung von Hardware-Komponenten weg. Andererseits lassen sich so auch flexibel die benötigten Volumen von Daten speichern und verarbeiten. Auch wenn die Technologien dahinter hochkomplex sind, sind heutige IaaS-Angebote relativ standardisiert verfügbar auf dem Markt.

So ist der Vendor Lock-in bei klassischen IaaS-Diensten überschaubar, da diese mit vertretbarem Aufwand ausgewechselt werden können. Dies führt dazu, dass sich die Angebote, rein ökonomisch betrachtet, nur noch durch den Preis differenzieren, da die technischen Leistungen klar spezifizierbar sind. Wenn jedoch auch andere Kriterien wie der oben genannte Aspekt der Vertrauenswürdigkeit oder der physische Besitz der Server berücksichtigt werden, so unterscheiden sich die Angebote auf dem Markt sofort wesentlich. Denn gemäss CLOUD Act (Clarifying Lawful Overseas Use of Data Act) Handhabung seit dem Schrems II Urteil können bspw. US-Behörden auf Daten auf Microsoft-Servern zugreifen, selbst wenn diese in Schweizer Rechenzentren stehen (Hildén, 2021). Auch können faktisch Regierungen die Aktivitäten von nationalen Unternehmen überwachen, wie dies bspw. die chinesische Regierung im Fall von Alibaba praktiziert (Keane & Yu, 2019). Dies führt dazu, dass auch bei IaaS-Angeboten im Sinne der digitalen Souveränität auf den geografischen Standort und die Eigentümerschaft geachtet werden sollte.

Dasselbe gilt für «Platform-as-a-Service» (PaaS) Angebote. Diese primär für Entwicklungsarbeiten genutzten Cloud-Services beschleunigen die moderne Software-Entwicklung und den Betrieb von komplexen Anwendungen wesentlich. Allerdings ist die Vielzahl der möglichen PaaS-Dienste so gross,

[23] https://www.swisscom.ch/de/business/enterprise/angebot/iot/lpn.html

[24] https://www.beesmart.org

dass auf dieser Schicht wiederum eine deutliche Gefahr des Vendor Lock-in besteht. So können heutige amerikanische und chinesische Hyperscaler spezialisierte und hoch performante PaaS-Dienste zu sehr günstigen Preisen anbieten, europäische Lösungen sind in der Regel deutlich teurer (Kagermann et al., 2021). In diesem Zusammenhang wurde 2021 im Rahmen von GAIA-X die Initiative «Sovereign Cloud Stack» (SCS)[25] in Deutschland lanciert. Diese Open Source-basierten Cloud-Technologien fokussieren auf die IaaS-Schicht, um damit standardisierte Services anbieten zu können (Kagermann et al., 2021).

In der Schweiz wiederum wurde 2020 die Idee einer sogenannten «Swiss Cloud» lanciert, aber nach einer Konsultationsrunde vorläufig wieder sistiert[26]. Die aktuelle Cloud-Strategie des Bundes sieht einen Hybrid Multi Cloud Ansatz vor, also dass sowohl interne Server als Private Cloud wie auch unterschiedliche Public Cloud Anbieter verwendet werden[27]. Nach der Vergabe der Public Cloud Ausschreibung an amerikanische und chinesische Hyperscaler im Sommer 2021 wurde die Thematik einer «Swiss Cloud» erneut aktuell[28]. In der Politik sind zwei gleichlautende parlamentarische Initiativen zur Schaffung einer eigenständigen digitalen Infrastruktur im vergangenen Jahr eingereicht worden.

Allerdings ist zu bemerken, dass die 2020 diskutierte «Swiss Cloud» im Wesentlichen eine staatliche IaaS-Lösung für die Schweizer Wirtschaft umfasst hätte, während dem sich die zurzeit diskutierte Variante einer «Swiss Cloud» primär von Schweizer IT-Firmen an Behörden richtet[29]. Diese Begriffsunklarheiten tragen aktuell dazu bei, dass immer wieder problematische Missverständnisse in entsprechenden Diskussionen auftreten.

3.3 Datenräume: Mobilität, Gesundheit, private Daten

Schichtenmodell Ebene 5

Der Begriff des Datenraums hat sich in jüngster Zeit in der datenpolitischen Literatur sowie in den digitalpolitischen Konzepten der Europäischen Kommission etabliert. Aus ökonomischer Sicht ist der Begriff der Datenallmende hilfreich (Bertschek et al., 2021). Das Angebot an Daten im digitalen Raum ist enorm, aber dennoch gibt es noch viele Daten, die nicht öffentlich zugänglich sind, obwohl ihre Verfügbarkeit hohen gesellschaftlichen Nutzen generieren würde. Bereits 2015 hat die Europäische Kommission in einem ausführlichen Bericht dargelegt, welchen Wert die Freigabe von Behördendaten als «Open Government Data» (OGD) mit sich bringt (Europäische Kommission, 2015). Der Report ging von einem direkten OGD Marktvolumen von 325 Milliarden Euro aus, die im Zeitraum von 2016 bis 2020 zu realisieren seien.

Besonders interessant erscheinen die Wertschöpfungspotenziale am Beispiel des Verkehrs; hier verlagern sich neue digitale Potenziale möglicher Plattformen für vernetzte Mobilität und Mobilitätsdienste. Die damit verbundenen Wertschöpfungspotenziale könnten mit einer Datenallmende weiter besser realisiert werden (Bertschek et al., 2021).

[25] https://scs.community/

[26] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-81573.html

[27] https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/cloud.html

[28] https://www.inside-it.ch/post/public-cloud-die-eidgenossenschaft-holt-chinesen-ins-land-20210624

[29] https://www.computerworld.ch/social/interview/schweiz-eigene-cloud-2749628.html

3.3.1 Mobilitätsdatenraum Schweiz – Nutzungsszenarien für «Mobility as a Service»

Bereits im Aufbau als Digitaler Service Public ist die Nationale Datenvernetzungsinfrastruktur Mobilität (NADIM). Der Bezug zum Gedanken eines neuen Angebots der Grundversorgung (Digitaler Service Public) ist in der Studie von ecoplan (2019) hinreichend diskutiert worden. Ein zusätzlicher, noch wenig beachteter Aspekt ist die Vorstellung von einer sozialen Teilhabe (beispielsweise an Mobilität). Mobilität wird häufig als Dichotomie öffentlicher Verkehr vs. Privatverkehr (motorisierter Individualverkehr MIV) betrachtet. Daubitz (2021) entwirft die Vision einer öffentlichen Mobilität jenseits dieser Dichotomie und entwickelt einen Ansatz, wonach Mobilität gesellschaftliche Teilhabe ermöglicht. Eine inklusive Verkehrsplanung könnte mit einem offenen Datenraum, der sämtliche Verkehrsträger umfasst, partizipativ angegangen werden; die Planung wäre nicht mehr alleinige Angelegenheit der Verkehrsplaner*innen und verkehrsanbietendenden Organisationen, sondern auch Bürger*innen könnten mit spezifischen Kompetenzen eine eigene Mobilitätsplanung machen, statt sich auf beherrschende Verkehrsanbieter verlassen zu müssen (Bundesministerium für Verkehr und digitale Infrastruktur, 2018).

Demand Responsive Transport (DRT) sind intelligente Verkehrssysteme, die auf spezifische Fahrtwünsche der Nutzer*innen reagieren können. Matchingsysteme ermöglichen beispielsweise die Bündelung der Fahrtwünsche von Taxifahrten. Das Teilen von Taxi-Diensten ist nicht nur günstiger, es sorgt ebenfalls für eine bessere Auslastung der physischen Infrastruktur (weniger Verkehrsaufkommen). Solche stark individualisierte Mobilitätskonzepte könnten sich beispielswiese auf einer Art «letzten Meile» im Verkehr als überlegen zu bisherigen Modellen (Service Public) erweisen. Mobility as a Service (MaaS) würde sogar eine höhere Dienstleistungsqualität als ein bestehendes öffentliches Angebot aufweisen; solche Szenarien sind allerdings nur umsetzbar, wenn «Dateneigentum und -nutzung der Verkehrsteilnehmer adäquat geregelt wird» (Lütjens et al., 2018). MaaS erfordert ein datengetriebenes Mobilitätsmanagement.

Der öffentliche Verkehr, der in der Schweiz gut ausgebaut und als Service Public breite Anerkennung geniesst, kann allerdings der Nutzer*innenorientierung und dem Bedürfnis nach individueller Mobilität nicht gerecht werden. Eine nutzerzentrierte Ausgestaltung von öffentlicher Mobilität – so die Hoffnung vieler Mobilitätsstudien – benötigt ein gutes Datenmanagement. Die Mobilitätsinfrastruktur weist eine digitale Dimension auf, damit mittels Echtzeit-Daten die Wahl des besten Verkehrsmittels möglich ist. Dank der Analyse vorhandener Datensätze eröffnen sich neue Chancen für Anbieter*innen in der Verkehrsplanung (Wolking, 2021).

3.3.2 Lücken in der Daten-Infrastruktur: Beispiel Gesundheitsdaten

Weniger weit fortgeschritten als bei der Mobilitätsdateninfrastruktur ist der Bereich der Gesundheitsdaten. Dies zeigen zwei Studien eindrücklich: Die Analyse von foraus und sensor advice (Knobel et al., 2020) als auch die neuere Version der Swiss Data Alliance (SDA) diskutieren die Defizite einer nationalen und international anschlussfähigen Dateninfrastruktur. Die SDA beklagt, dass die Schweiz «zurzeit keine kohärente Strategie (kennt), ein digitales und vernetztes Gesundheitsdatenökosystem aufzubauen» (Früh et al., 2022; Swiss Data Alliance, 2021); in der foraus-Studie wird ebenfalls beklagt, es fehle in der Schweiz an einer einem gemeinsamen Verständnis im

Umgang mit Gesundheitsdaten auf globaler Ebene aufgrund unterschiedlicher Wertesysteme, es mangle an einer Datenkompetenz in der Bevölkerung und es bestehe fehlende Wahrnehmung des Mehrwerts von Gesundheitsdaten für die öffentliche Gesundheit. Für den Service Public-Gedanken relevant ist die Benennung einer «mangelnden Finanzierung technischer Systeme und Dateninfrastrukturen zur grenzüberschreitenden Nutzung und Austausch von Gesundheitsdaten», weiter fehle es an «einheitlichen Dateninfrastrukturen und Standards für den barrierefreien nationalen und internationalen Austausch von Gesundheitsdaten». Der foraus-Brief empfiehlt deshalb eine «nachhaltige Finanzierung technischer Dateninfrastrukturen, die den Austausch und die Nutzung von Gesundheitsdaten ermöglichen» (Knobel et al., 2020, S. 47) Auch wenn nicht explizit Bezug genommen wird auf einen Digitalen Service Public, so werden doch sämtliche Bestandteile beklagt (Marktversagen) bzw. die Vorstellung von Gesundheitsdaten als öffentliches Gut propagiert.

3.3.3 Das ungenutzte Potential der privaten Daten von öffentlichem Interesse

Von Privaten erzeugte (nicht-personenbezogene) Daten sind ein ungenutztes Potenzial für die Gesellschaft. Die EU-Kommission stellt im Entwurf zum «Data Act» die Regeln für die Datennutzung, die Bedingungen für den Zugang durch öffentliche Einrichtungen, internationale Datenübertragungen, Cloud-Switching und Interoperabilität zur Diskussion. In der Pressemitteilung für das «Datengesetz» wird explizit auf den Charakter von Daten als öffentliches Gut Bezug genommen.[30] Mit dem Data Act will die Kommission das Potenzial der datengesteuerten Innovation freisetzen. Dies umfasst auch vernetzte Geräte (Internet of Things). Erstmals soll Nutzern ein Zugang zu denjenigen Daten ermöglicht werden, welche sie mit ihrer Nutzung selbst erzeugt haben. Der Data Act sieht auch eine Regelung des Cloud-Switching vor. Wenn jemand eine Software oder eine Anwendung von einem Cloud-Dienst zu einem anderen verlagern will, kommt er in den Genuss der «funktionalen Äquivalenz». Dies zwingt die Anbieter, die Kompatibilität mit offenen Standards oder Interoperabilitäts-Schnittstellen zu garantieren. Die Kommission sieht dafür Normungsorganisationen vor, welche die Interoperabilität von Cloud-Diensten normieren würden. Für die Durchsetzung sind die zuständigen Behörden der Mitgliedsstaaten zuständig.

Auch in der Schweiz wird der Wert von Daten immer mehr erkannt. Einerseits hat der Bundesrat Anfang 2022 im Bereich der Digitalisierungsaktivitäten als erstes Thema den Schwerpunkt «Vertrauenswürdige Datenräume» festgelegt[31]. Dabei soll die Vereinbarkeit von digitaler Selbstbestimmung und gemeinsamer Datennutzung im Vordergrund stehen. Andererseits befindet sich seit Februar 2022 mit dem «Bundesgesetz über die Mobilitätsdateninfrastruktur» (MODIG) erstmals ein sektorspezifisches Datengesetz in der Vernehmlassung. Dessen Ziel ist es, die Datennutzung zwischen Staat und Unternehmen zu verbessern, um letztlich das Verkehrswachstum besser zu bewältigen[32]. Ein wichtiger Bestandteil der Vorlage umfasst die Freigabe der Kerndaten als OGD: kostenlos verfügbar, in

[30] «Daten zeichnen sich ebenso wie Musikaufnahmen, Strassenbeleuchtung oder eine malerische Aussicht durch Nicht-Rivalität aus, was bedeutet, dass viele Menschen gleichzeitig Zugang dazu haben und sie immer wieder „konsumiert" werden können, ohne dass ihre Qualität darunter leidet oder sie zur Neige gehen. https://ec.europa.eu/commission/presscorner/detail/de/ip_22_1113 .

[31] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87029.html

[32] https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87009.html

maschinenlesbarer Form und in einem offenen Format zur freien Weiterverwendung. Die in der Botschaft detailliert umschriebenen Kerndaten umfassen Geodaten, Verkehrsdaten, Betriebsdaten sowie Teile der Vertriebsdaten[33]. Ausserdem sollen über sogenannte «Open Services» auch konkrete Datenabfragen ermöglicht werden, wie z.B. ein Routing-Service, der den optimalen Pfad zwischen zwei Punkten ergibt. Die Bereitstellung der OGD und diese Open Services werden auf der nationalen Datenvernetzungsinfrastruktur Mobilität (NADIM) betrieben, die ein integrierter Bestandteil der Mobilitätsdateninfrastruktur darstellt.

In der Botschaft zum MODIG ist ebenfalls übergreifend beschrieben, weshalb der Staat diesen Service Public im digitalen Raum erbringen soll: Der öffentlich finanzierte Aufbau und Betrieb der NADIM reduziert einerseits das Risiko von Effizienzverlusten aufgrund unterschiedlicher technischer Standards und die Monopolbildung von privaten Akteuren, die aufgrund des Vendor Lock-ins in der Informatikbranche oftmals ein Problem darstellen. Andererseits nützt die staatliche Digitalinfrastruktur allen, da aufgrund von Marktversagen gewisse Daten und Dienste nicht zur Verfügung stünden oder nicht die notwendige Qualität und Diskriminierungsfreiheit bieten würden.

Die Integration sektorspezifischer Datenräume in gesamteuropäische Datenräume müsste von Beginn weg beachtet werden. Die Schweiz sollte dabei die EU-Standards von Beginn weg übernehmen, weil die Verflechtung über den Binnenmarkt ohnehin schon eng ist (Swiss Data Alliance, 2021).

3.3.4 Crowd-sourced Data

Parallel zu staatlichen Digitalangeboten werden insbesondere in der zivilgesellschaftlichen Digitalszene häufig Plattformen durch Crowd-Sourcing Ansätzen aufgebaut. So ist Wikipedia heute eine aktuelle, weit verbreitete und zuverlässige Informationsquelle zu zahlreichen Wissensgebieten und neusten Entwicklungen. Gleichzeitig wurden in den letzten 18 Jahren mit OpenStreetMap grosse Datenmengen an nutzergenerierte Geoinformationen erarbeitet, die heute auf einer Vielzahl von Anwendungen integriert sind (Bernard et al., 2019).

Immer häufiger entdecken heute staatliche Stellen das Potential von Open Source Software oder Crowd-sourced-Plattformen. So kooperierten beispielsweise swisstopo mit Geoinformationsbehörden aus anderen Ländern, sowie privaten Open Source Anbietern, im Rahmen von Open Source Crowdfunding-Ansätzen, um benötigte Software für die staatliche Geoinfrastruktur weiterzuentwickeln.[34] Oder das BAV liess zusammen mit SBB und swisstopo abklären, ob und wie Geodaten aus dem Geoportal des Bundes in OpenStreetMap wiederverwendet werden können und umgekehrt (Hitz-Gamper & Stürmer, 2021).

3.4 Softwaretechnologien

Schichtenmodell Ebene 6

[33] Bundesrat, 2022. Bundesgesetz über die Mobilitätsdateninfrastruktur - Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens. https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen.msg-id-87009.html

[34] https://www.geo.admin.ch/de/news/aktuell.detail.news.html/geo-internet/news2019/news20190115.html

Öffentlich finanzierte Softwaretechnologien werden grundsätzlich für die Erfüllung staatlicher Aufgaben entwickelt. So beschaffen Bund, Kantone und Gemeinden für rund 3 Milliarden Franken pro Jahr Informatikleistungen[35], die vorwiegend für die interne Anwendung genutzt werden. Die Veröffentlichung von Software für die Bevölkerung hat in der Vergangenheit nicht zum Service Public des Staates gehört, ausser wenn es um die Erfüllung gesetzlich geregelter Dienste ging, wie bspw. das Ausfüllen der Steuererklärung (TaxMe) oder um Covid-Zertifikate während der Pandemie (Covid-App).

Wenn jedoch Daten als digitale Infrastruktur verstanden werden und ein Digitaler Service Public dazu aufgebaut werden soll (siehe vorherigen Abschnitt), ist es entscheidend zu verstehen, dass Daten ohne Software weder genutzt, gespeichert, verarbeitet noch dargestellt werden können. Die Nutzung von Daten setzt Online- oder Offline-Applikationen voraus, mit denen Dokumente und andere Daten bearbeitet werden können.

So wird beispielsweise für die Erstellung eines Textdokuments ein Textverarbeitungsprogramm benötigt, heute typischerweise Microsoft Word. Es bestehen zwar Alternativen, aber die sind aufgrund des Netzwerkeffekts von Datenstandards und Gewohnheiten der Bevölkerung wenig verbreitet. Heute kann Word noch lokal auf Computer verwendet werden, aber Microsoft priorisiert die Cloud-Variante 365 und wird möglicherweise die on-premise Version bald ganz ablösen[36]. So werden die privaten Nutzenden und auch Behörden und Firmen bald nicht mehr nur von der Software, sondern auch auf Seiten der Daten abhängig von Microsoft sein.

Dieser Vendor Lock-in äussert sich auch darin, dass bei Informatikbeschaffungen überdurchschnittlich viele überschwellige freihändige Vergaben (Aufträge über CHF 230'000 ohne öffentliche Ausschreibung) stattfinden (Stuermer et al., 2017). Gemäss aktuellen Statistiken liegt der Durchschnitt von Freihändern bei rund 20% von allen Beschaffungen, bei Informatikzuschlägen ist der Freihänder-Anteil bei rund 45%, die Tendenz in den letzten fünf Jahren ist sogar steigend[37].

Mit diesem Verlust an digitaler Souveränität sind in diesem Beispiel zwei der drei Kriterien betroffen, die für einen künftigen digitalen Service Public sprechen: Einerseits ist die Wahlfreiheit eingeschränkt, da häufig keine valablen Alternativen bspw. zu Microsoft Office bestehen. Andererseits ist die Vertrauenswürdigkeit fraglich, da bspw. über den CLOUD Act die amerikanische Regierung Zugriff auf private Daten erhalten kann.

Dieses Beispiel zeigt auf, weshalb auch bei Softwaretechnologien ein staatlicher Eingriff gerechtfertigt sein kann. Eine Möglichkeit stellt dabei die Förderung von Open Source Software dar, da diese die digitale Souveränität von Individuen und Behörden erhöht. Der Zugang zum Quellcode schafft Unabhängigkeit von den Herstellern, sodass die Software-Nutzenden die Rahmenbedingungen selbständig bestimmen können, wie die Software betrieben und weiterentwickelt wird. Insbesondere kann der Staat die strategische Ausrichtung der Vergabeverfahren auf die Beschaffung von Open Source Software ausrichten, um Hersteller-Abhängigkeiten zu reduzieren.

[35] https://intelliprocure.ch/beschaffungen-statistik

[36] https://www.heise.de/meinung/Analyse-Azure-und-365-als-einzige-Microsoft-Zukunft-6178614.html

[37] https://intelliprocure.ch/dashboard

3.4.1 EMBaG, Open Source, digitales Covid-Zertifikat

Mit dem neuen «Bundesgesetz über den Einsatz elektronischer Mittel zur Erfüllung von Behördenaufgaben» (EMBaG) sollen unter anderem die gesetzlichen Grundlagen für die Freigabe von Open Source Software (Art. 10 VE-EMBaG) und Open Government Data (Art. 11 VE-EMBaG) gelegt werden. Dadurch wird klargestellt, dass Bundesbehörden Open Source Software entwickeln und publizieren dürfen. Auch wenn gute Gründe dafür bestehen, dass dies ohne explizite gesetzliche Grundlage schon bisher zulässig war, ist die Frage umstritten, wie mehrere Gutachten aufzeigten (Müller & Vogel, 2014) (Poledna et al., 2017). Schon heute veröffentlichen zahlreiche Bundesämter wie swisstopo[38], MeteoSchweiz[39] und das Bundesamt für Informatik und Telekommunikation (BIT)[40] auf Open Source Entwicklungs-Plattformen wie GitHub laufend neu Software-Komponenten unter Open Source Lizenzen. Insgesamt wurden so in den letzten Jahren von mehreren Bundesämtern über 150 Open Source Module (Repositories) veröffentlicht.[41] Unter anderem hat das BIT beispielsweise die über 20 Software-Komponenten publiziert, welche die Ausstellung und Kontrolle der Covid-Zertifikate gewährleisten[42].

Insgesamt zeigt die rasche Entwicklung und der zuverlässige Betrieb des Covid-Zertifikats exemplarisch auf, welche Vorteile eine staatliche Informatikinfrastruktur und die entsprechende Erfahrung in der Software-Entwicklung durch die öffentliche Hand mit sich bringt: So konnten das Bundesamt für Gesundheit (BAG), Bundesamt für Bauten und Logistik (BBL) und das BIT in Zusammenarbeit mit externen Firmen in kürzester Zeit eine solide und sichere Software-Lösung entwickeln, die (zumindest von der technischen Seite) das Vertrauen der Bevölkerung geniesst[43].

Dass der Staat die nicht-personenbezogenen Daten zugänglich macht, wäre eigentlich eine Selbstverständlichkeit. Dennoch hat es den Behörden oft an genügendem Durchsetzungswillen gefehlt, um ein Bewusstsein für eine OGD-Kultur aufzubauen, Kellerhals spricht pointiert von «unverbindlicher Verbindlichkeit» im real gelebten Open-Government-Data Alltag (Kellerhals, 2018). Mit dem EMBaG soll nun dem OGD-Gedanken verbindlich und eindeutig nachgeholfen werden. Beklagt wird allerdings, dass die Verwaltungseinheiten nicht verpflichtet sind, die Daten zum Zweck der Veröffentlichung auf Richtigkeit, Vollständigkeit, Plausibilität oder in sonstiger Weise zu prüfen (Früh et al., 2022).

3.4.2 Staatliche Förderung von Open Source Software

Software, die unter einer von der Open Source-Initiative ratifizierten Lizenz[44] veröffentlicht ist, wird als «Open Source Software» bezeichnet. Alle diese über 100 Lizenzen geben unter anderem vor, dass die entsprechend lizenzierte Software beliebig eingesetzt, verändert und weiterverbreitet werden darf. Dies ist möglich, da die Lizenz Einblick in den Quellcode der Software gewährleistet. Damit ist sichergestellt, dass sowohl aus rechtlicher wie auch aus technischer Perspektive vollständiger Zugriff auf das geistige Eigentum besteht und dessen Nutzung in keiner Weise eingeschränkt wird. Ist die Open Source Software

[38] https://github.com/geoadmin
[39] https://github.com/MeteoSwiss-APN
[40] https://github.com/admin-ch
[41] https://ossbenchmark.com/institutions
[42] https://github.com/orgs/admin-ch/repositories
[43] https://www.bit.admin.ch/bit/de/home/themen/stories/covid-zertifikat.html
[44] https://opensource.org/licenses/alphabetical

auf dem Internet veröffentlicht, können alle auf die entsprechenden Elemente zugreifen und wiederverwenden.

Die staatliche Freigabe von Open Source Software stellt nur ein Beispiel dar, wie Behörden einen konkreten Service Public im digitalen Raum erbringen können. Da Open Source Software als öffentliches, digitales Gut gilt (Johnson, 2002; Sahay, 2019), können bei einer Veröffentlichung alle davon profitieren – andere Behörden, Bildungs- und Forschungsinstitutionen, Unternehmen, Vereine, Privatpersonen etc. So lassen sich Software-Lösungen, die einmal von einer öffentlichen Stelle entwickelt wurden, von anderen Behörden wiederverwenden. Gleichzeitig können beliebige IT-Anbieter kommerzielle Dienstleistungen wie Wartung, Weiterentwicklung, Betrieb, Schulungen etc. erbringen, ohne dass ein Vendor Lock-in entsteht. Denn typische Open Source Lizenzen geben vor, dass alle Erweiterungen auch wieder als Open Source Software freigegeben werden müssen, sodass der öffentliche Zugang langfristig verfügbar ist.

Problematisch ist es, wenn Open Source-Anwendungen und -Komponenten an geschäftskritischen Stellen eingesetzt werden, aber deren Sicherheit nicht gewährleistet ist. So wurde 2014 eine gefährliche Sicherheitslücke in der Open Source Kryptografie-Komponente OpenSSL entdeckt, die damals in rund einer halben Million Servern im Einsatz war (Durumeric et al., 11052014). Dieser sogenannte «Heartbleed» Fehler wurde rasch behoben, jedoch entstanden Schäden durch Hacker-Angriffe und Wartungsarbeiten von schätzungsweise mehreren hundert Millionen US-Dollar.[45] Mit solchen Schwächen in zentralen Open Source-Komponenten muss vermehrt gerechnet werden, da sie an vielen Stellen im öffentlichen Sektor und in der Privatwirtschaft eingesetzt werden. Erst Ende 2021 wurde erneut eine Sicherheitslücke entdeckt, dieses Mal in der Open Source Komponente log4j.[46] Es wird angenommen, dass bei dieser Lücke namens «Log4Shell» gar mehrere hundert Millionen Geräte betroffen sind, und diese teilweise noch jahrelang unsicher im Internet zugänglich sein werden.[47]

Als Service Public im digitalen Raum hat deshalb die Europäische Kommission 2017 das Programm «Free and Open Source Software Auditing» (EU-FOSSA) lanciert, über das bis 2020 insgesamt 200'000 Euro für gefundene Fehler und deren Korrektur an Open Source-Entwickler ausbezahlt wurden.[48] Ein Neustart des Programms ist im Januar 2022 angekündigt worden, womit nun Sicherheitslücken in weit verbreiteten Applikationen wie LibreOffice und Odoo gefunden und geschlossen werden sollen.[49]

In der Schweiz verantwortet der Bereich «Digitale Transformation und IKT-Lenkung» die Vorgaben bezüglich Open Source-Software-Nutzung in der Bundesverwaltung. Mit einem strategischen Leitfaden und einem Praxis-Leitfaden werden Bundesstellen bei konkreten operativen Fragestellungen zum Open Source-Einsatz unterstützt.[50]

[45] https://www.eweek.com/security/heartbleed-ssl-flaw-s-true-cost-will-take-time-to-tally/

[46] https://www.cyberscoop.com/log4j-cisa-easterly-most-serious/

[47] https://www.wired.com/story/log4j-log4shell/

[48] https://ec.europa.eu/info/news/eu-fossa-2-eus-open-source-cybersecurity-project-ends-2020-jul-14_en

[49] https://ec.europa.eu/info/news/european-commissions-open-source-programme-office-starts-bug-bounties-2022-jan-19_en

[50] https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software.html

Auf politischer Ebene wird mit dem EMBaG (siehe oben Abschnitt 3.4.1) nun auch die Freigabe von Open Source Software auf eine gesetzliche Grundlage gestellt. Gleichzeitig praktizieren bereits seit mehreren Jahren zahlreiche Bundesämter die Veröffentlichung von Open Source-Software auf GitHub und anderen Plattformen; dies stellt heute in der Informatik eine Selbstverständlichkeit dar. Bestimmte Anwendungen wie die Swiss Covid App oder die Covid-Zertifikat App wurden von Anfang unter Open Source-Lizenzen veröffentlicht.

Potential gibt es in der Schweiz von staatlicher Seite noch bezüglich expliziter Förderung von Open Source-Entwicklungen. So könnten Bundesstellen, interkantonale Gremien und Städteverbände eine aktive Koordinationsrolle übernehmen, um die gemeinsame Entwicklung von Behörden-Lösungen zu unterstützen. Erste Ansätze sind schon vorhanden, beispielsweise stellt der Verein «inosca» eine interkantonale Entwicklungsgemeinschaft für elektronische Bewilligungsprozesse dar[51].

3.5 Rechts- und Wertesystem

Schichtenmodell Ebene 7

Die letzte Ebene im Schichtenmodell thematisiert das Rechts- und Wertesystem. Kagermann et al., 2021 verstehen darunter die Fähigkeit «inwiefern es gelingt, europäische Grundüberzeugungen und Werte in konkrete Spielregeln für den europäischen Binnenmarkt zu übersetzen» (S. 27). Sie verengen den Blick dann allerdings auf Cybersicherheit. An dieser Stelle wird die Perspektive aber geöffnet.

Die in der Verfassung und im Völkerrecht verankerten Grundrechte können Abwehransprüche, Leistungsansprüche oder Schutzansprüche enthalten. Häufig verbinden sie auch mehrere dieser Anspruchsarten (Kiener et al., 2018). Im digitalen Zeitalter entstehen neue Gefährdungen und damit auch neue Schutzansprüche bzw. – aus der Perspektive des Staates – Schutzpflichten. Nachfolgend werden Regulierungsvorschläge für einen besseren Schutz der Grundrechte im digitalen Zeitalter aufgeführt. Einige der Regulierungsvorschläge finden sich auch bei Busch, wobei dort unklar bleibt, weshalb der Staat in diesen Bereichen regulieren soll. Busch zeigt zwar auf, dass sich die Plattformisierung von Wirtschaft und Gesellschaft nicht allein als Wettbewerbsproblem erfassen lässt. Er stellt fest, das Digitalkonzerne in Lebensbereiche vordringen, in denen es um gesellschaftliche Teilhabe, Demokratie und die Grundversorgung der Bevölkerung mit wesentlichen Leistungen geht und nimmt den Medienstaatsvertrag als Beispiel dafür, «dass der wettbewerbsrechtliche Rahmen durch zusätzliche Regelungen ergänzt werden muss, die auch andere gesellschaftlich relevante Regelungsziele berücksichtigen» (Busch, 2021, S. 21). Es bleibt jedoch unklar, warum es diese ergänzenden Regelungen braucht. Nachfolgend wird gezeigt, dass neue Regelungen deshalb erforderlich sind, weil nur so die bereits in der Verfassung verankerten Grundrechte auch im digitalen Zeitalter ihre Wirkung entfalten können.

3.5.1 Plattformregulierung und Digital Services Act

Wenn Plattformanbieter Konsument*innen diskriminieren, gäbe es rechtliche Möglichkeiten, diese sind allerdings lückenhaft. Gegen viele dieser Einschränkungen stehen schon heute rechtliche Instrumente

[51] https://inosca.ch

zur Verfügung. So kann beispielsweise das Aussperren aus dem App-Store als Missbrauch einer marktbeherrschenden Stellung von Art. 7 des Kartellgesetzes erfasst werden (konkret: Verweigerung von Geschäftsbeziehungen gemäss Art. 7 Abs. 2 lit. a KG). Jedoch hat sich die Wettbewerbskommission bisher in erster Linie auf Fälle mit Beteiligung von schweizerischen Unternehmen konzentriert. In diesem Beispiel ist auch ein zivilrechtliches Vorgehen mit grossen Schwierigkeiten verbunden, angefangen beim möglicherweise fehlenden Gerichtsstand in der Schweiz bis hin zur Kostenfrage. Unternehmen wie Google und Facebook leisten sich in der Regel die teuersten Anwälte, dementsprechend ist das Kostenrisiko auch dann hoch, wenn ein Gerichtsstand in der Schweiz gegeben ist und die Verfahrenskosten selbst noch überschaubar wären. Ob das schweizerische Recht die oben genannten Grundrechte durch entsprechende Gesetzgebung besser gewährleisten will, ist eine politische Frage. Wenn sie mit Ja beantwortet wird, können die im Kapitel 3.5 aufgeführten Regulierungsvorschläge herangezogen werden.

Digitale Souveränität meint auf staatlicher Ebene die Kontrolle über Entscheidungsfindung und die Umsetzung von Dienstleistungen zu erhalten (Kagermann et al. 2021). Dies ist keine Selbstverständlichkeit, denn proprietäre Technologien führen häufig zu technologischen Blockaden und Silos (Kagermann et al. 2021). Digitale öffentliche Güter wie Open Source-Software ermöglichen es den Ländern, Technologien so zu übernehmen, anzupassen und zu skalieren, dass ihre Flexibilität erhalten bleibt. Mit der zunehmenden Verbreitung digitaler öffentlicher Güter – und damit der digitalen Souveränität – entstehen neue Formen der Zusammenarbeit (OECD, 2021).

Die Frage, ob private Plattformen stärker reguliert werden sollen, ist von der Politik zu beantworten. Wenn sie bejaht wird, bieten die geltenden Gesetze jedoch nur wenig Handhabe. Das schweizerische Kartellrecht hat im Bereich der Fusionskontrolle im Hinblick auf grosse internationale Konzerne keine ernstzunehmende Wirkung. Aber auch beim Tatbestand des Missbrauchs einer marktbeherrschenden Stellung, hat die Wettbewerbskommission bisher keine Verfahren gegen Unternehmen wie Alphabet (Google), Meta (Facebook), Amazon oder Apple geführt. Das Verhalten dieser Unternehmen ist in der Regel nicht unlauter im Sinne des Gesetzes gegen den unlauteren Wettbewerb (UWG). Wenn eine stärkere Regulierung grosser Softwarekonzerne ins Auge gefasst werden soll, erscheint es daher naheliegend, sich am in Entstehung befindlichen EU-Gesetz über digitale Dienste (Digital Services Act) zu orientieren.

Das Europäische Parlament hat am 20. Januar 2022 den Bericht zum Vorschlag für dieses Gesetz beschlossen, der Bericht wird nun im Trilog zwischen Parlament, Rat und Kommission verhandelt. Das Gesetz unterscheidet zwischen Vermittlungsdiensten, Hosting-Diensten und Online-Plattformen, wobei für sehr grosse Online-Plattformen (damit gemeint sind Plattformen, die mehr als 10 % der 450 Millionen Verbraucher*innen in Europa erreichen) besondere Regeln gelten. Die Erfahrung zeigt allerdings, dass sich Unternehmen wie Alphabet (Google), Meta (Facebook) und Amazon für ihre Tätigkeit in Europa am EU-Recht orientieren und die entsprechenden Regeln im gesamten europäischen Raum, d.h. auch in der Schweiz, umsetzen. Beispielhaft kann hier auf die Folgen des Urteils des EuGH zum Recht auf Vergessen hingewiesen werden. Google hat die darin aufgestellten Anforderungen im gesamten europäischen Raum umgesetzt, obwohl es rechtlich zulässig gewesen wäre, in der Schweiz vorerst nichts zu ändern. Vor diesem Hintergrund ist fraglich, ob schweizerisches Recht überhaupt noch einen entscheidenden Einfluss auf das Verhalten der dominanten Anbieter hat.

3.5.2 Regulierungsvorschläge für einen verbesserten Schutz der Meinungs- und Informationsfreiheit

Die Meinungs- und Informationsfreiheit wird heute zunehmend auch durch private Plattformen eingeschränkt. Wenn das Twitter-Konto einer Politikerin gesperrt wird, kann das einschneidende Konsequenzen, bis hin zur Gefährdung einer Wiederwahl, mit sich bringen. Das heutige Rechtssystem bietet aber kaum Möglichkeiten, um gegen eine solche Sperrung vorzugehen. In den privatrechtlichen Verträgen bzw. Nutzungsbestimmungen steht, dass die Plattformen ihr Angebot jederzeit und ohne Angabe von Gründen einstellen oder anpassen dürfen. Solche Bestimmungen sind üblich und in der Schweiz grundsätzlich auch rechtskonform. Es ist nicht davon auszugehen, dass ein Gericht in der Schweiz wie der deutsche Bundesgerichtshof entscheidet und Grundrechte wie die Meinungsfreiheit auch gegenüber privaten Unternehmen wie Meta (Facebook) anwendet (Urteil des Bundesgerichtshofs III ZR 179/20 vom 29. Juli 2021).

Wenn essenzielle Kommunikationsplattformen zur Einhaltung gewisser Mindeststandards verpflichtet werden sollen, sind diese Mindeststandards gesetzlich festzulegen. Weil auf EU-Ebene bereits Regulierungsbestrebungen in diese Richtung laufen, kann es durchaus sein, dass Plattformbetreiber die entsprechenden Regeln zukünftig in ganz Europa und damit auch in der Schweiz beachten. Dies war bereits bei der Umsetzung der Vorgaben des EuGH im Fall Google gegen Mario Costeja zu beobachten (Urteil des EuGH C-131/12 vom 13. Mai 2014, Google Spain SL und Google Inc. gegen Agencia Española de Protección de Datos [AEPD] und Mario Costeja González). So würde die Schweiz erneut von EU-Regulierung profitieren, ohne in die Entstehung dieser Regeln involviert zu sein.

Regulierungsbestrebungen in diese Richtung finden sich insbesondere in Art. 12 Abs. 2 des Vorschlags für ein EU-Gesetz über digitale Dienste. Dieser lautet wie folgt: «Die Anbieter von Vermittlungsdiensten gehen bei der Anwendung und Durchsetzung der in Absatz 1 genannten Beschränkungen sorgfältig, objektiv und verhältnismäßig vor und berücksichtigen dabei die Rechte und berechtigten Interessen aller Beteiligten sowie die geltenden Grundrechte der Nutzer, die in der Charta verankert sind.»

3.5.3 Regulierungsvorschläge für einen verbesserten Schutz der Privatsphäre

Der Schutz der Privatsphäre ist in Art. 13 BV verankert. Zum Schutz der Privatsphäre hat das eidgenössische Parlament das eidgenössische Datenschutzgesetz erlassen, zudem haben sämtliche Kantonsparlamente je ein kantonales Datenschutzgesetz (teilweise kombiniert mit anderen Themen, z.B. Informations- und Datenschutzgesetz in Basel und Zürich) erlassen. Diese Gesetze verhindern nicht, dass zum Beispiel in Schulen Software eingesetzt wird, die es dem Softwarehersteller erlaubt, personalisierte Daten jeder Schülerin und jedes Schülers zu erheben und auszuwerten. Häufig sehen die Nutzungsbestimmungen dieser Produkte vor, dass das Aufzeichnen und Auswerten dieser Daten erlaubt ist. Die Schülerinnen und Schüler haben faktisch häufig keine Wahl (Becker, 2017)[52] und lesen die Nutzungsbestimmungen, wie auch alle anderen Nutzerinnen und Nutzer, in der Regel nicht.

Wenn zum besseren Schutz der Privatsphäre von Schüler*innen verhindert werden soll, dass personalisierte Daten aufgezeichnet und ausgewertet werden, sollte dies auf Gesetzesstufe geregelt

[52] «Die take it or leave it-Situation der Einwilligung».

werden. Merkblätter von Datenschutzbeauftragten oder von privaten Vereinigungen (wie zum Beispiel Privatim) sind rechtlich unverbindlich und zudem demokratisch nicht legitimiert.

Eine Möglichkeit zum besseren Schutz der Privatsphäre wäre die Schaffung eines Rechts auf datenerhebungsfreie Produkte (Becker, 2017). Ein solches wurde auch schon in der sogenannten «Charta der Digitalen Grundrechte der Europäischen Union» aufgenommen. Der Titel dieses Dokuments ist jedoch irreführend, da es nicht von der EU stammt, sondern auf Initiative von Netzaktivist*innen, Politiker*innen, Wissenschaftler*innen, Schriftsteller*innen, Journalist*innen und Bürgerrechtler*innen unter dem Dach der Zeit-Stiftung erarbeitet worden ist[53]. Nichtsdestotrotz wäre die Einführung eines solchen Rechts im Hinblick auf einen verbesserten Schutz der Privatsphäre eine Möglichkeit, um die Überwachung von Schüler*innen im obligatorischen Schulunterricht zu verhindern.

3.5.4 Regulierungsvorschläge für einen verbesserten Schutz der Wirtschaftsfreiheit

Abhängig von Grösse und Branche, können Unternehmen darauf angewiesen sein, in Suchmaschinen zu erscheinen. Dies kann im Rahmen der normalen Suche oder in Form von bezahlter Werbung oder auch auf beiden Wegen wichtig sein. Als Beispiel kann der Fall der Ant IT herangezogen werden. In der NZZ wurde der Fall wie folgt geschildert:

> «Lieber Google-Ads-Kunde, mindestens eine Ihrer Anzeigen oder eines Ihrer Keywords wurde abgelehnt.» Als Ivan Bonassi am 16. Mai von Google angeschrieben wird, versteht er die Welt nicht mehr. Seit drei Jahren bewirbt der Zürcher IT-Supporter und PC-Reparateur seine Ein-Mann-Firma Ant IT in den Suchresultaten von Google: Wer nach «PC-Reparatur Zürich» und dergleichen googelt, ist oft auf seine Anzeigen gestossen.
>
> […]
>
> Die im Silicon Valley beschlossene Änderung hat für sein Geschäft im Zürcher Kreis 6 gravierende Konsequenzen: «Dank Google hatte ich vier bis fünf Neukunden pro Woche. Jetzt ist das Telefon tot, von einem Tag auf den nächsten.» Dabei hat er erst vor einem Monat seinen kleinen neuen Reparaturladen am Schaffhauserplatz eröffnet.
>
> Quelle: NZZ vom 8. Juni 2019, S. 17[54]

Dieser Fall zeigt exemplarisch, welche Auswirkungen eine Änderung an einem Algorithmus einer grossen Suchmaschine für ein Unternehmen haben kann. Wenn Unternehmen von der Auffindbarkeit via Suchmaschinen abhängig sind, könnte der Staat für einen verbesserten Schutz der Wirtschaftsfreiheit aktiv werden. Anforderungen an die Transparenz von Suchmaschinen-Algorithmen würden jedoch in die Wirtschaftsfreiheit der Suchmaschinenbetreiber eingreifen, und sind deshalb kritisch zu beurteilen. Der Staat könnte jedoch dafür sorgen, dass bereits bestehendes Recht tatsächlich durchgesetzt werden kann. Der oben beschriebene Sachverhalt dürfte den im Kartellgesetz verankerten Tatbestand des Missbrauchs einer marktbeherrschenden Stellung erfüllen. Dasselbe gilt auch für die Nichtaufnahme von Apps in den App-Stores der Anbieter von Mobiltelefon-Betriebssystemen.

[53] Siehe https://digitalcharta.eu/hintergrund/ sowie https://digitalcharta.eu/intiatorinnen-und-initiatoren/.

[54] Google-Suche: Firma für IT-Support in Zürich darf nicht werben (nzz.ch)

Gegen solche missbräuchlichen Verhaltensweisen könnte einerseits die Weko vorgehen, andererseits steht auch der zivilrechtliche Weg offen. Trotzdem ist ein erfolgreiches Vorgehen gegen eine grosse Suchmaschine mit sehr hohen Hürden verbunden. Vertreter der Wettbewerbskommission haben sich wiederholt dahingehend geäussert, dass sie ein Vorgehen gegen internationale Unternehmen der EU-Kommission überlassen[55]. Gleichzeitig ist auch der zivilrechtliche Weg mit hohen Hürden verbunden. Dies auch deshalb, weil marktmächtige Unternehmen in der Regel sehr gut bezahlte Anwält*innen einsetzen, was das Kostenrisiko für die Gegenseite noch zusätzlich in die Höhe treibt[56].

Um dem materiellen Recht (hier: Kartellgesetz) zum Durchbruch zu verhelfen und die Ansprüche nicht nur in der Theorie zu gewähren, könnte der Staat das Kostenrisiko für die Rechtsdurchsetzung senken. Dies wäre beispielsweise im Rahmen der laufenden ZPO-Revision, in der dieses Thema bereits enthalten ist, möglich. Dem SDA-Bericht zur parlamentarischen Debatte vom 16. Juni 2021[57] ist zu entnehmen: «Ziel der Reform der Zivilprozessordnung ist es, Privaten und Unternehmen der Zugang zu Gerichten zu erleichtern. Unter anderem soll er dafür das Prozesskostenrecht angepasst werden.»

3.5.5 Regulierungsvorschläge für einen verbesserten Schutz des Rechts auf Teilhabe am wissenschaftlichen Fortschritt

Gemäss Art. 15 Abs. 1 lit. b des internationalen Pakts über wirtschaftliche, soziale und kulturelle Rechte (UNO-Pakt I; in Kraft getreten für die Schweiz am 18. September 1992) erkennen die Vertragsstaaten das Recht eines jeden an, an den Errungenschaften des wissenschaftlichen Fortschritts und seiner Anwendung teilzuhaben. Die UN-Sonderberichterstatterin für kulturelle Rechte hat im Jahr 2014 im 24-seitigen Bericht «Copyright policy & the right to science and culture» aufgezeigt, wie Staaten dieses Recht konkret gewährleisten können. In den Empfehlungen am Ende des Berichts ist ein Abschnitt dem Thema «Adopting policies fostering access to science and culture» gewidmet. Eine der dort aufgelisteten Empfehlungen lautet wie folgt: «The products of creative efforts subsidized by governments, intergovernmental organizations or charitable entities, should be made widely accessible. States should redirect financial support from proprietary publishing models to open publishing models»[58].

In der Schweiz haben bisher der Schweizer Nationalfonds (SNF) und swissuniversities Vorgaben betreffend offene Publikationsmodelle erlassen. Während die Vorgaben des SNF teilweise verbindlich sind, indem sie zur Voraussetzung für die Forschungsfinanzierung gemacht wurden, kann swissuniversities als Zusammenschluss der Hochschulen in Form eines Vereins keine Vorgaben erlassen, die für die Hochschulen verbindlich sind. Zwar hat sich swissuniversities das Ziel gesetzt, dass bis 2024 alle staatlich finanzierten wissenschaftlichen Publikationen frei zugänglich sein sollen, es ist

[55] Aus einem Interview mit dem WEKO-Präsidenten Andreas Heinemann (NZZ vom 2. Juni 2018): «Häufig signalisieren grosse Internetfirmen, dass sie die mit der EU vereinbarten Lösungen auch auf die Schweiz anwenden. Wir greifen einen Fall nur auf, wenn es spezifische Aspekte für die Schweiz gibt.» Aus einem Interview mit dem Weko-Direktor Patrik Ducrey (SRF Online vom 28. Juni 2017): «Wir hatten im Oktober 2015 ebenfalls eine Vorabklärung gegen Google eröffnet. Wir haben diese aber sistiert, weil wir den Entscheid der EU-Kommission abwarten wollten.»

[56] Dem Entscheid B-3238/2021 des Bundesverwaltungsgerichts vom 18. Oktober 2021 ist beispielsweise zu entnehmen, dass Google von der Anwaltskanzlei Homburger AG vertreten wird.

[57] SDA-Meldung vom 16. Juni 2021 (Ständerat schraubt in Zivilprozessordnung an Medienfreiheit).

[58] Bericht der UN-Sonderberichterstatterin für kulturelle Rechte, Copyright policy and the right to science and culture, Ziff. 112.

aber schon heute klar, dass dieses Ziel nicht erreicht wird. Das liegt u.a. daran, dass swissuniversities lediglich Empfehlungen erlassen kann und es den einzelnen Hochschulen überlassen bleibt, ob und ggf. wann sie diese umsetzen. Hinzu kommt, dass sich viele Wissenschaftler*innen aus ganz unterschiedlichen Gründen gegen eine Pflicht zum offenen Publizieren wehren. So hat beispielsweise die rechtswissenschaftliche Fakultät der Universität Zürich eine von der Universitätsleitung vorgeschlagene verbindliche Formulierung mit dem Argument abgelehnt, dass die Universität keine rechtliche Grundlage für eine solche Vorgabe habe[59]. Aber auch die (verbindlichen) Vorgaben des SNF werden unter Berufung auf die Wissenschaftsfreiheit vonseiten der Rechtswissenschaft teilweise als Eingriff in die Forschungsfreiheit betrachtet (Erass, 2020), die im Gesetz selbst zu regeln seien (Erass, 2020).

Diese Beispiele zeigen, dass die von der UN-Sonderberichterstatterin für kulturelle Rechte empfohlenen Vorgaben zumindest in den Grundzügen vom Gesetzgeber und nicht (nur) von den Hochschulen oder swissuniversities zu erlassen sind. Dementsprechend ist zu empfehlen, im Bundesgesetz über die Förderung der Hochschulen und die Koordination im schweizerischen Hochschulbereich eine gesetzliche Grundlage für offene Publikationsmodelle einzufügen. Diese sollte nicht ausschliesslich Open Access (d.h. die offene Publikation von wissenschaftlicher Literatur), sondern auch Open Educational Resources (d.h. insbesondere Lehrbücher) und Open Research Data erfassen[60].

3.5.6 Regulierungsvorschläge für einen verbesserten Schutz gegen Diskriminierung

Vorbemerkung: Mit Diskriminierung ist hier der verfassungsrechtliche Diskriminierungsbegriff (Art. 8 Abs. 2 BV) gemeint. In nicht-juristischen Kreisen und in anderen Jurisdiktionen wird der Begriff häufig breiter verstanden. So zielen beispielsweise die Regeln zur Diskriminierungsfreiheit von Medienintermediären in § 94 des deutschen Medienstaatsvertrags nicht gegen eine Diskriminierung im Sinne von Art. 8 BV, sondern gegen eine Abweichung von den im Sinne der Transparenzpflicht (§ 93 Medienstaatsvertrag) umschriebenen Algorithmen.

Gemäss Art. 8 Abs. 2 BV darf niemand diskriminiert werden, namentlich nicht wegen der Herkunft, der Rasse, des Geschlechts, des Alters, der Sprache, der sozialen Stellung, der Lebensform, der religiösen, weltanschaulichen oder politischen Überzeugung oder wegen einer körperlichen, geistigen oder psychischen Behinderung. Immer dann, wenn eine Ungleichbehandlung ohne sachlichen Grund an einem dieser Merkmale anknüpft, liegt eine verbotene Diskriminierung vor.

Im digitalen Zeitalter verschiebt sich ein immer grösserer Teil der menschlichen Aktivitäten in den digitalen Raum. Viele Angebote sind von Grund auf rein digitale Angebote, die nur für Menschen zugänglich sind, welche einerseits über die nötige Infrastruktur (Internetzugang, Hardware, Software) und andererseits über das notwendige Knowhow verfügen. Der Staat muss nicht dafür sorgen, dass genuin digitale Angebote auch analog zugänglich sind. Eine Diskriminierung kann aber dann vorliegen,

[59] Diese Information findet sich in einem Tweet des Open-Science-Beauftragten der Universität Zürich, Prof. Mark Robinson. Er schreibt: «There were also some legal questions. We (intentionally?) worded the initial draft of the OS Policy as *requirements*. The UZH Faculty of Law (among others) emphatically pointed out that 'you do not have the legal basis to force us'.» (https://twitter.com/markrobinsonca/status/1465759502377046026 | archiviert: https://perma.cc/625V-HTDM).

[60] Bericht der UN-Sonderberichterstatterin für kulturelle Rechte, Copyright policy and the right to science and culture, Ziff. 111.

wenn staatliche Leistungen wie z.B. ein Formular für das Beantragen von Ergänzungsleistungen vorschnell nur noch ausschliesslich digital angeboten werden. Bei Menschen, die Ergänzungsleistungen beantragen, handelt es sich häufig um ältere Menschen oder auch um Menschen mit einer psychischen oder körperlichen Beeinträchtigung. Bei älteren Menschen ist die Computer- und Internetnutzung heute noch signifikant weniger verbreitet als bei jüngeren. Rein digitale Angebote können diesen Teil der Bevölkerung ausschliessen. Um dieser Gefahr zuvorzukommen, könnte gesetzlich festgeschrieben werden, dass der Staat gewährleistet, dass auch Menschen, denen die Infrastruktur oder das Knowhow fehlt, nicht von staatlichen Leistungen ausgeschlossen werden. Das muss nicht heissen, dass nicht mehr zeitgemässe analoge Prozesse weiterbetrieben werden müssen. Es ist auch möglich, dieser Personengruppe anzubieten, mit menschlicher Unterstützung gemeinsam ein Formular an einem Behörden-PC auszufüllen. Das Bundesgericht hat diesbezüglich in seinem Urteil 1C_137/2018 Urteil vom 27. November 2018 festgehalten: "Der Staat ist daher gehalten, insofern in vernünftigem Rahmen Ausweichmöglichkeiten vorzusehen, wo die Beschränkung des Zugangs zu staatlichen Aktivitäten oder Informationen im Ergebnis zu einem Verlust der Teilhabe der Betroffenen insbesondere an staatlichen Entscheiden und Leistungen und damit zu einer Ausgrenzung führen kann." Im konkreten Fall hat das Bundesgericht in der Umstellung auf eine ausschliesslich elektronische Publikation des Amtsblattes des Kantons Zürich keine Altersdiskriminierung erkannt.

In den letzten Jahren sind im Bereich von Deep Learning und Natural Language Processing enorme Fortschritte erzielt worden. Diese Technologien basieren auf der Auswertung grosser Datenmengen, wobei die genaue Funktionsweise häufig nicht im Detail nachvollzogen werden kann. Dies kann dazu führen, dass in den Trainingsdaten enthaltene diskriminierende Elemente zu einer weiteren Diskriminierung durch Algorithmen führen. In der Schweiz ist die Diskriminierung durch Unternehmen nur dann unzulässig, wenn es sich um eine Diskriminierung aufgrund des Geschlechts (GlG) oder um eine Diskriminierung aufgrund einer Behinderung handelt. Mit Blick auf die möglicherweise wachsende Gefahr von allen möglichen Formen von Diskriminierungen durch Private sollte vertieft geprüft werden, ob der Zeitpunkt für ein allgemeines Diskriminierungsgesetz gekommen ist.

3.5.7 Regulierungsvorschläge für einen verbesserten Schutz der Verfahrensgarantien

Gemäss Art. 30 Abs. 3 BV sind Gerichtsverhandlung und Urteilsverkündung öffentlich. In der vordigitalen Zeit war die mündliche Verkündung von Urteilen kombiniert mit der schriftlichen Publikation von Leitentscheiden des höchsten Gerichts die naheliegendste Möglichkeit zur Umsetzung der von der Verfassung geforderten Justizöffentlichkeit. Parallel zur stetigen Ausbreitung des Internets ist das Bundesgericht dazu übergegangen zunächst nur die Leitentscheide[61], später auch einzelne weitere Urteile und schliesslich sämtliche Urteile auf seiner Webseite zu publizieren[62]. In der vordigitalen Welt hätte die Publikation sämtlicher Urteile einerseits zu einer Papierflut und andererseits zu einer kaum bewältigbaren Informationsüberflutung geführt. In der digitalen Welt jedoch nicht mehr. In den Kantonen wurde mit grosser Zurückhaltung begonnen, ebenfalls einzelne Urteile und im Laufe der Zeit mehr und mehr Urteile zu publizieren. Heute werden in etwa sieben Kantonen alle Urteile der obersten

[61] Tschümperlin, S. 73.

[62] Tschümperlin, S. 75.

kantonalen Instanz(en) publiziert, in allen anderen Kantonen eine Auswahl. Bei den erstinstanzlichen Urteilen sind die Unterschiede noch grösser: In einigen Kantonen werden bis heute gar keine erstinstanzlichen Urteile publiziert, in anderen nur wenige und in ganz wenigen Kantonen werden die meisten erstinstanzlichen Urteile online veröffentlicht. Dies führt dazu, dass nicht nur 26 (jeder Kanton) plus 4 (alle Gerichte des Bundes) auf je einer eigenen Webseite Urteile publizieren. In vielen Kantonen werden die Urteile verschiedener Gerichte auf verschiedenen Seiten und teilweise mit unterschiedlichen Systemen publiziert (Guyan, 2018). Für die Rechtssuchenden hat dies bis vor Kurzem bedeutet, dass sie bei einer allgemeinen Recherche entweder in über 50 verschiedenen Datenbanken suchen mussten, oder dass sie für den Zugang zu staatlicher Information auf private Anbieter zurückgreifen und dort für den Zugang zur Information hohe Kosten bezahlen mussten. Dieser Umstand hat dazu geführt, dass sich ein privater Verein dieser öffentlichen Aufgabe angenommen hat. Dieser betreibt eine frei zugängliche Webseite, auf der alle von kantonalen Gerichten oder von Gerichten des Bundes publizierten Entscheide zentral durchsuchbar und abrufbar sind (www.entscheidsuche.ch).

Im November 2020 hat der Bundesrat den Vorentwurf zu einem Bundesgesetz über die Plattform für die elektronische Kommunikation in der Justiz (BEKJ) in die Vernehmlassung geschickt[63]. Mit Blick auf die von der Verfassung geforderten Justizöffentlichkeit erscheint naheliegend, in einer E-Justiz-Plattform auch die Urteilspublikation zu integrieren und dies im Gesetz vorzusehen. Nachdem das Thema im Vorentwurf nicht enthalten war, ist im Hinblick auf den Entwurf zuhanden des Parlaments zu empfehlen, die Urteilspublikation im Gesetz aufzunehmen[64].

[63] Medienmitteilung des Bundesrates vom 11. November 2020: Bundesrat schlägt zentrale Plattform für den elektronischen Rechtsverkehr vor.

[64] Dies wurde auch in den Vernehmlassungsantworten von verschiedenen Parteien gefordert: Vernehmlassungsantwort der FDP, S. 2; Vernehmlassungsantwort der GLP, S.3 ; Vernehmlassungsantwort der Mitte, S. 2; Vernehmlassungsantwort der SP, S. 2.

Tabelle 2 Das Technologie-Schichtenmodell nach Kagermann et al., (2021), im Kontext der Herausforderungen für den Schweizer DSP

	Ebene (nach Kagermann et al.)	**Bestandteile / Fokusbereich (nach Kagermann et al.)**	**Schweizer DSP (Herausforderungen)**
7	Europäisches Rechts- und Wertesystem	Cybersecurity, Kryptografie, E-Identity, EU-Zertifizierung (Verbraucherschutz) und Standards	MODIG, EMBaG, Grundrechte und staatliche Schutzpflichten
6	Softwaretechnologien	App-Entwicklungen, Office, ERP, KI, Middleware, Robotik-Software, Blockchain, Algorithmen, EU- Open Source, VR/AR, QC	Veröffentlichungen von OSS (Swiss Covid Zertifikat) auf GitHub, Strategischer Leitfaden und Praxisleitfaden OSS
5	Europäische Datenräume	Zum Beispiel für Mobilität, Health, Public Sector, digitaler öffentlicher Raum	NADIM, opendata.swiss, OGD Strategie Bund, Open Street Map
4	Platform-as-a-Service (PaaS)	Anwendungs- und Entwicklungsökosysteme B2B und B2C (Abstraction Layer, Container Technology) QC, KI, IoT	BIT Atlantica Cloud
3	Infrastructure-as-a-Service (IaaS)	Virtuelle, verteilte Cloud-Ökosysteme, Edge-Technologie, QC, KI-HPC-Center	BIT Atlantica Cloud
2	Kommunikationsinfrastruktur	Breitbandinfrastruktur, Mobilfunknetze (Open RAN), Galileo-Navigation	LoRaWAN, The Things Network
1	Komponenten	Mikrochips, Sensoren, Aktuatoren, Fertigungs- und Basistechnologien, 3D-Druck, QC, KI	
0	Rohmaterialien und Vorprodukte	Seltene Erden	

4 Diskussion des Konzepts «Government as a Platform (GaaP)»

Der Staat ist mit vielen neuen Herausforderungen konfrontiert, welche ihren Ursprung darin haben, dass der Technologiefortschritt immer schneller immer weitreichendere Folgen zeitigt – vor allem, aber nicht nur, der Fortschritt in der Informationstechnologie und in der Gentechnologie. Das Konzept Government as a Platform (GaaP) adressiert dieses Anwachsen der Herausforderungen. Es wurde ursprünglich von Tim O'Reilly populär gemacht und wird mittlerweile von Institutionen und Autoren auf sehr unterschiedliche Weise interpretiert. Beispielsweise formuliert die OECD: «A government acts as a platform for meeting the needs of users when it provides clear and transparent sources of guidelines, tools, data and software that equip teams to deliver user-driven, consistent, seamless, integrated, proactive and cross-sectoral service delivery" (OECD, 2020), um dann den Schluss abzuleiten, dass GaaP entweder ein Ökosystem sein kann, oder ein Marktplatz, oder eine Neudefinition der Beziehungen zwischen Einwohner*innen und Staat. Wir haben es im Wesentlichen mit mindestens zwölf Arten von kritischen Ressourcen zu tun, welche benötigt werden, damit der Staat seine Aufgaben mit digitalen Hilfsmitteln zeitgemäss wahrnehmen kann: Expert*innen, Kooperationsräume, Vertrauensinfrastruktur, digitale Wissens- und Informationsressourcen, Interoperabilitätsstandards (im Sinne des EIF[65], potentiell inklusive zertifizierter APIs), vertrauenswürdige Infrastruktur zum Datenteilen für Schlüsselbereiche von Wirtschaft und Gesellschaft, Qualitätsmanagementinstrumente, Datenräume, digitale Lösungsbausteine, Instrumente zur institutionellen Unterstützung für die gesellschaftliche Teilhabe, sowie Instrumente zur institutionellen Unterstützung für die politische Teilhabe.

Wir werden uns im Folgenden auf drei dieser zehn kritischen Ressourcen konzentrieren:

1. *Vertrauensinfrastruktur*: Infrastruktur für das Ökosystem der verifizierbaren digitalen Zertifikate inklusive einer Implementierung der digitalen Brieftasche und der internationalen Vernetzung;
2. Instrumente zur institutionellen *Unterstützung für die gesellschaftliche Teilhabe*: staatliche Dienstleistungen, welche Menschen helfen, die Schwierigkeit mit Online-Aktivitäten haben oder Opfer von solchen wurden;
3. *Digitale Lösungsbausteine*: Software-Komponenten, Prozess-Komponenten, Service-Komponenten und die jeweils entsprechenden APIs, welche für das Bauen von Lösungen genutzt werden können, sowie die Verzeichnisdienste zum Auffinden dieser Lösungsbausteine und Brokerdienste.

4.1 Vertrauensinfrastruktur

Für eine Vertrauensinfrastruktur sollten verschiedene Prinzipien erfüllt sein, damit sie die digitale Souveränität auf individueller Ebene garantiert:

- Sie ermöglicht es, überprüfbare Aussagen mit digitalen Mitteln zu machen, und trägt so zur Schaffung von Vertrauenswürdigkeit bei, was wiederum das Vertrauen in digitale Interaktionsräume stärkt.

[65] New European Interoperability Framework, EU Commission 2017

- Die Kontrolle über das Generieren von digital überprüfbaren Aussagen liegt bei den Institutionen, welche die Gültigkeit der Aussagen mit ihrer Glaubwürdigkeit bestätigen.
- Die Kontrolle über die Informationsflüsse liegt bei der/dem jeweils Betroffenen. Sie/er entscheidet, wer welche der über sie/ihn der generierten Aussagen enthält.
- Die Aussagen können im Inland wie zumindest auch im europäischen Ausland für Online-Aktivitäten genutzt werden.
- Ein Teil dieser überprüfbaren Aussagen kommt vom Staat und bildet das Fundament für den Aufbau eines digitalen Ökosystems – konkret Aussagen zur Identität einer Person oder einer Organisation.
- Ein Teil dieser überprüfbaren Aussagen kommt von Institutionen, deren Identität und institutionelle Natur durch den Staat überprüfbar bestätigt wird – das Ökosystem ist als beliebig erweiterbar designt und deckt einen grossen Teil der wichtigsten Eigenschaftsnachweise ab.
- Die technische Qualität des Ökosystems garantiert seine Cybersicherheit. Und für den Fall, dass solche Angriffe trotzdem gelingen, gibt es eine umfassende, beratende, technische und rechtliche Unterstützung.
- Das technische Design setzt Datensparsamkeit im maximalen Ausmass um, so dass bei der Nutzung nur jene Informationen generiert werden, die zwingend notwendig sind.
- Das Ökosystem ist einfach verständlich, erlaubt auch ohne Fachwissen eine sichere Nutzung und ergänzend können Nutzer*innen ohne grossen Aufwand fachliche Unterstützung bekommen. Zudem ist es für alle Einwohner*innen erschwinglich.

Eine Möglichkeit, solch eine Vertrauensinfrastruktur zu bauen, stellen Self Sovereign Identities (SSI[66]) Zertifikate (respektive Credentials) dar, mit denen man ein verteiltes und damit dezentrales Ökosystem an überprüfbar-vertrauenswürdigen Eigenschaftsbeweisen bauen kann. Sie können von ihren Besitzern (respektive Holder) in einem Digital Wallet aufbewahrt und jenen gezeigt werden, welche einen vertrauenswürdigen Beweis dieser Eigenschaften bekommen wollen – und zwar ohne, dass die Aussteller der Zertifikate dies erfahren. Dabei bleibt die Kontrolle über die Zertifikate uneingeschränkt bei deren Besitzern, das heisst jenen, auf die sich die Aussage im Zertifikat bezieht.

Wesentlich für einen erfolgreichen Aufbau eines solchen Ökosystems ist, dass für Aussteller, Überprüfer und Besitzer der digital überprüfbaren Zertifikate das Ökosystem als Ganzes nicht nur ein vertrauenswürdiges Überprüfen von Aussagen ermöglicht, sondern dadurch so viel Nutzen bringt, dass sie bereit sind, die Anfangsinvestitionen zu tätigen.

Aus den obigen Überlegungen folgt auch,

a. dass es keine privatwirtschaftliche Lösung geben kann, weil der Vertrauensanker vom Staat kommen muss;
b. dass der Aufbau einer Vertrauensinfrastruktur ein gesamtgesellschaftliches Vorhaben ist – insbesondere, weil das System nur funktioniert, wenn es genutzt wird und es nur genutzt wird, wenn es viele Nutzungsmöglichkeiten gibt;

[66] Self-Sovereign Identity (SSI) 101: Decentralized Identifiers (DIDs) & Verifiable Credentials (VCs) (gataca.io), W3C Konsortium

c. dass die Rolle des Staats einerseits über das Ausgeben einer eID hinausgehen, anderseits aber beschränkt bleiben muss: Das Ökosystem braucht Nutzungsmöglichkeit der Zertifikate im E-Government, damit die Attraktivität für die Nutzenden erhöht wird, aber es braucht auch Nutzungsmöglichkeiten in der Privatwirtschaft, die privatwirtschaftlicher Logik folgen.

Deshalb ist die Vertrauensinfrastruktur ein natürlicher Kandidat für einen digitalen Service Public, dessen Governance aber nur in Zusammenarbeit mit der Wirtschaft[67] erarbeitet werden kann.

4.2 Instrumente zur Unterstützung der gesellschaftlichen Teilhabe

Die gesellschaftliche Teilhabe wird durch Wissens- und Knowhow-Defizite, ökonomisch beschränkten Zugang zu digitalen Ressourcen, das Fehlen einer Vertrauensinfrastruktur und durch Cybergefahren eingeschränkt. Staatsaufgaben in der Ausbildung werden hier nicht diskutiert. Ebenso wenig die ökonomischen Aspekte. Die oben besprochene Vertrauensinfrastruktur ist ein konstruktives Element, das alle zur Teilhabe befähigt. Der Schutz vor Cybergefahren ist dagegen ein separates Thema, welches im Folgenden besprochen wird.

Wir sind derzeit mit einer unübersichtlichen und sich schnell verändernden Sachlage in Bezug auf Cybergefahren konfrontiert, welche auch für Fachkräfte oft die Einordnung konkreter Gefahren oder Schutzmassnahmen schwer macht. Im Fall konkreter Angriffe sind viele Privatpersonen und auch Unternehmen überfordert. Sicherheit verlangt aktive Wahrnehmung der Eigenverantwortung, doch ist diese nur notwendig, aber nicht hinreichend. Das staatliche Handeln konzentriert sich derzeit sehr stark auf den Schutz der kritischen Infrastruktur. Die Unterstützung beim Selbstschutz vor Cybergefahren ist dagegen eine Privataufgabe.

Tatsächlich zeigt sich aber in diversen Studien, dass selbst viele Behörden die Einwohner*innen durch mangelhafte technische Lösungen dem Tracking durch nicht sichtbare Unternehmen aussetzen[68]. Der Staat schützt also nicht nur die Bewohner*innen nicht, er gefährdet sie in einigen europäischen Ländern sogar potenziell. Dazu gab es in der Schweiz in letzter Zeit vermehrt Berichte über erfolgreiche Cyberangriffe auf Gemeinden[69]. Deshalb sollte darüber nachgedacht werden, wie Menschen und Organisationen besser sowohl beim proaktiven Selbstschutz als auch beim reaktiven Beseitigen der Schäden von Angriffen durch den Staat unterstützt werden könnten. Eine Option wäre ein staatliches Cybersicherheitsportal, welches Informationen, Werkzeuge und im Falle von Angriffen Hilfedienstleistungen anbietet. Solch ein Portal hätte den positiven Nebeneffekt, dass die Bereitschaft zum Melden viel grösser wäre als bisher, weil es mehr bietet als eine Bestätigungsmail, dass die Meldung ankam.

[67] Vergleiche dazu das dänische Kooperationskonzept für NEmID und MitID: From NemID to MitID: All You Need to Know | Penneo

[68] EU government websites infested with third-party adtech scripts | ZDNet

[69] Z.B. Hacker veröffentlichen GB an vertraulichen Daten der Gemeinde Rolle VD (watson.ch)

4.3 Digitale Lösungsbausteine

Ein wesentlicher Grund für die Rückständigkeit der Schweizer Verwaltung im E-Government ist, dass bislang stets die Entscheidung lautete, keine Lösungsbausteine für alle zur Verfügung zu stellen. Namentlich beim Thema IAM (Identity and Access Management) wurde dies in den letzten Jahren in den Gremien des E-Government mehrfach diskutiert und die Kantone wurden dazu befragt. Trotz eines klaren Wunsches vieler nach zentral bereitgestellten Lösungen, entschied man sich bislang immer dagegen. Im Ausland wurde diesbezüglich eine wesentlich andere Praxis verfolgt.

Sowohl die EU-Kommission als auch einzelne EU-Mitgliedstaaten, entwickelten IAM-Module als Open Source Software, welche einfach in Anwendungen integrierbar sind. Auf nationaler Ebene hat dies wesentlich zum Erfolg der eID in einigen Ländern beigetragen. Auf internationaler Ebene schuf es die Grundlagen für den Aufbau des Netzwerks zur grenzüberschreitenden Nutzung nationaler eIDs in der EU. Deshalb plant die EU-Kommission auch für die vorgeschlagene Umsetzung der Weiterentwicklung der eIDAS Regulierung[70] eine Open Source Lösung für das Digital Wallet bereitzustellen.

Um die Innovation im E-Government zu beschleunigen, erscheint es deshalb sinnvoll, die Kosten für sie durch das Prinzip «einmal entwickeln, vielfach nutzen» zu reduzieren. Gute, erprobte Lösungen immer wieder neu ein erstes Mal zu bauen, führt nicht nur zu hohen Kosten, sondern schafft auch das Risiko, dass schlechte Lösungen entwickelt werden, wo bessere bereits existieren. Die Joinup-Platform der EU[71] versucht deshalb das Teilen zu fördern. Aus Sicht von E-Government Dienstleistungsanbietern ohne viel IT-Wissen ist diese europäische Plattform jedoch kaum nutzbar. In vielen Bereichen sind insbesondere die nationalen Unterschiede zu gross, um ausländische Lösungen wiederverwenden zu können. Innerhalb der Schweiz wäre eine Wiederverwendung viel einfacher möglich – auch dort, wo Kantone oder Gemeinden unterschiedliche Gesetze haben. Es ist deshalb realistisch, eine Plattform von qualitätsgeprüften E-Government Lösungsbausteinen zu schaffen, welche schweizweit von Gemeinden und Kantonen genutzt werden kann. Diese würde deren Kosten für Innovationen im E-Government verringern und damit den Fortschritt beschleunigen.

[70] Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität

[71] Joinup (europa.eu)

5 Ergebnisse im Überblick

Kapitel 5 ist unterteilt in drei Abschnitte: Abschnitt 5.1 zeigt neue Aufgaben und Regulierungen in Bezug auf einen digitalen Service Public auf, strukturiert nach der Rolle des Staates (Anbieter, Regulator oder Förderer von digitalen Gütern, Services oder Infrastrukturen). Abschnitt 5.2 beinhaltet Empfehlungen, und Abschnitt 5.3 umfasst ein Fazit mit weiterführenden Überlegungen zu einem Digitalen Service Public.

5.1 Digitaler Service Public: Neue Aufgaben und Regulierungen

Nachfolgend aufgelistet werden Massnahmen, welche der Grundversorgung oder der digitalen Souveränität dienen. Wir sehen aufgrund der Diskussionen im europäischen Umfeld und der in der Literatur diskutierten Probleme einen Digitalen Service Public unter folgenden Bedingungen als erforderlich, wenn:

- aufgrund der Public-Good-Eigenschaften **kein Anbieter auf dem Markt** ein gesellschaftlich erwünschtes Gut produziert;
- Individuen oder der Staat **Abhängigkeiten von privaten Anbietern** ausgesetzt sind, welche hohe Kosten verursachen, oder;
- das **Vertrauen** in einen Dienst nicht vorhanden ist, weil Daten preisgegeben werden, über die man nur **mangelhafte Kontrolle** hat.

Grundsätzlich gibt es zwei Möglichkeiten, diesem Marktversagen zu begegnen. Erstens, indem der Staat selbst ein Angebot zur Verfügung stellt, zweitens, indem er bestehende private Angebote im Sinne einer besseren Allokation der Ressourcen reguliert.

5.1.1 Der Staat als Anbieter von digitalen Gütern, Services und Infrastrukturen

Nachfolgend aufgelistet werden Massnahmen, welche der Grundversorgung oder der digitalen Souveränität dienen, sowie in Klammern die Begründung der Erforderlichkeit (siehe 5.1).

Der Aufbau von sektorspezifischen Datenräumen (Infrastruktur und Governance) braucht den Staat in der Rolle als Erbringer einer Dateninfrastruktur, weil die Kosten für die Infrastrukturleistungen niemand übernimmt. Diese Datenräume gehören zur Grundversorgung, ihnen wird ein hohes Innovationspotenzial zugetraut. Damit der Nutzen noch höher ist, sollten beim Aufbau die Standards auf europäischer Ebene von Anfang an übernommen werden (→ **kein Anbieter auf dem Markt**).

Bereits auf dem Weg ist die konsequente Umsetzung der offenen Behördendaten (open-by-default). Im EMBaG sind die gesetzlichen Grundlagen für die Open Government Data gelegt. Hier tritt der Staat als Anbieter der eigenen Daten auf. Der Public Service liegt im Bereitstellen der Daten auf einer zentralen Plattform für offene Verwaltungsdaten (→ **kein Anbieter auf dem Markt**).

Zur Grundversorgung des Staates kann man auch eine digitale Basisinfrastruktur für Cloud-Services zählen, um der Abhängigkeit von Hyperscalern zu entgehen. Auch aus der Perspektive der digitalen Souveränität liesse sich eine Public Cloud begründen. Der Staat kann eine solche Basisinfrastruktur

selbst erstellen oder erstellen zu lassen,[72] jedenfalls sollte eine solche Cloud-Lösung mit den europäischen Entwicklungen (GAIA-X) koordiniert werden (→ **mangelndes Vertrauen und Kontrolle**).

Um die digitale Souveränität zu stärken, kann der Staat als Beschaffer im Bereich der Software vermehrt auf Open Source Software setzen, welche von anderen Behörden wiederverwendet werden können. Das EMBaG hat die Grundlage für Freigabe von Open Source Software für den Bund geschaffen (→ **Abhängigkeiten von privaten Anbietern).**

5.1.2 Der Staat als Regulator von digitalen Gütern, Services und Infrastrukturen

Nachfolgend aufgelistet werden Massnahmen, welche mittels Regulierung der digitalen Souveränität dienen, sowie in Klammern die Begründung der Erforderlichkeit (siehe Einleitung 5.1).

Wenn die Politik private Plattformen im Sinne der digitalen Souveränität regeln soll, braucht es neue Regulierungen. Das schweizerische Kartellrecht hat im Bereich der Fusionskontrolle im Hinblick auf grosse internationale Konzerne keine ernstzunehmende Wirkung; eine stärkere Regulierung bedeutet, sich am EU-Gesetz über digitale Dienste (Digital Services Act) zu orientieren (→ **Abhängigkeiten von privaten Anbietern).**

Das Problem des Vendor Lock-in bei Clouddiensten schränkt die Wahlfreiheit ein und führt zu hohen switching costs. Eine Erhöhung der digitalen Souveränität erfordert Lösungsansätze über eine Regulierung; diese sind in der EU weit fortgeschritten, weshalb sich die Schweiz am Digital Data Act orientieren kann (→ **Abhängigkeiten von privaten Anbietern).**

Open Source Software Entwicklungen, welche vom Staat in Auftrag gegeben werden, können mit dem neuen EMBaG freigegeben werden; hingegen wächst mit zunehmender Verbreitung von OSS auch die Gefahr von Sicherheitslücken. Hier könnten die Behörden ihren Beitrag leisten, indem sie sich an internationalen Initiativen beteiligen und deren Sicherheit-Standards übernehmen (→ **mangelndes Vertrauen und Kontrolle**).

Um die bestehende Grundversorgung in kritischen Aufgabengebieten besser durchführen können, ist es denkbar, dass sie auf die Nutzung von Daten Privater zugreifen dürfen. In der Europäischen Union sieht der Data Act vor, dass im Falle eines aussergewöhnlichen Ereignisses (z.B. Pandemien oder Naturkatastrophen) der Staat diese Daten einfordern kann (→ **kein Anbieter auf dem Markt**).

5.1.3 Der Staat als Förderer von privaten gemeinwirtschaftlichen digitalen Gütern, Services und Infrastrukturen

Internet of Things (IoT)-Anwendungen benötigen Netzwerkinfrastrukturen, welche über den Bereich des FMG hinausgehen. Zum Beispiel «Long Range Wide Area Networks» (LoRaWAN) werden von privaten Anbietern aufgebaut. Es braucht den Staat nicht als Anbieter solcher Netzwerke, er könnte sich aber an den Kosten vom «The Things Network» beteiligen (→ **ungedeckte Kosten von privaten Anbietern auf dem Markt).**

[72] Die äussert komplexe Frage ist auch politisch umstritten und wird auch im Bericht «Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung» diskutiert (Collova et al. (2022); UVEK und EDA (2022))

Private Initiativen wie OpenStreetMap werden in Kooperationen mit staatlichen Behörden eingebunden. Solche Initiativen müssen weder vom Staat reguliert noch selbst angeboten werden, hingegen wäre es wünschenswert, wenn die Offenheit bei den Behörden gegenüber diesen Initiativen als zu nutzendes Kooperationspotenzial stärker genutzt würde **(→ Kein Problem).**

5.2 Empfehlungen

5.2.1 Zu Technologie & Daten

Im EMBaG-Entwurf werden wichtige gesetzlich Grundlagen für die Freigabe von Software und Daten geschaffen. Auch wenn dabei in beiden Fällen eine «open by default» Vorgabe eingeführt wird, heisst dies noch lange nicht, dass diese auch systematisch umgesetzt wird bzw. werden kann. Folgende Empfehlungen zielen darauf ab, dass die Freigabe von staatlicher Software und Behördendaten auch tatsächlich umgesetzt wird und so einen relevanten Beitrag im künftigen digitalen Service Public leisten kann:

- Die Erarbeitung eines Leitfadens zur Beschaffung von IT-Mitteln unter Berücksichtigung von Open Source Software (bspw. durch die Beschaffungskonferenz des Bundes BKB[73]) erhöht die digitale Souveränität in der öffentlichen Informatik und ermöglicht die spätere Freigabe als Open Source Software gemäss EMBaG.
- Wissen und Erfahrung in der öffentlichen Verwaltung im Umgang mit Open Source Software werden mittels internen und externen Weiterbildungen, sowie interaktiven Austauschmöglichkeiten (Arbeitsgruppen, Workshops, Konferenzen etc.) gefördert.
- Die Schaffung einer offiziellen Kompetenzstelle zu Open Source Software innerhalb einer geeigneten Verwaltungseinheit (bspw. beim Bundesamt für Informatik und Telekommunikation) unterstützt bei technischen und rechtlichen Fragestellungen und fördert und moderiert die Freigabe von Open Source Software. Diese Stelle ist künftig zuständig für die Umsetzung des bestehenden Strategischen Leitfadens und des Praxisleitfadens zu Open Source Software[74].
- Ein regelmässig erscheinender Bericht überwacht die Umsetzung der strategischen Vorgaben betreffend Open Source Software und zeigt u.a. auf, wie sich die Anzahl IT-Freihänder entwickelt.
- Eine umfassende Studie zum ökonomischen Nutzen durch die Freigabe von Open Source Software und Open Government Data zeigt das volkswirtschaftliche Potential des digitalen Service Public im Software- und Datenumfeld auf.

5.2.2 Zum Schutz der Grundrechte im digitalen Zeitalter

Im Abschnitt 3.5 wurde gezeigt, dass aus den Grundrechten staatliche Schutzpflichten fliessen und dass der Staat im digitalen Zeitalter neue Regeln zum Schutz der «alten» Grundrechte erlassen muss.

[73] https://www.bkb.admin.ch/bkb/de/home/bkb/empfehlungen.html

[74] https://www.bk.admin.ch/bk/de/home/digitale-transformation-ikt-lenkung/bundesarchitektur/open_source_software.html

- Zum besseren Schutz der Meinungs- und Informationsfreiheit könnte die Schweiz in Anlehnung an den Vorschlag für ein EU-Gesetz über digitale Dienste ein ähnliches Gesetz erlassen.
- Zum besseren Schutz der Privatsphäre könnte die Schweiz in einem bestehenden oder einem neu zu schaffendem Gesetz ein Recht auf datenerhebungsfreie Produkte verankern.
- Zum besseren Schutz der Wirtschaftsfreiheit könnte die Schweiz das Kostenrisiko für die Durchsetzung bereits bestehenden Rechts senken.
- Zum besseren Schutz des Rechts auf Teilhabe am wissenschaftlichen Fortschritt könnte die Schweiz im Bundesgesetz über die Förderung der Hochschulen und die Koordination im schweizerischen Hochschulbereich eine gesetzliche Grundlage für offene Publikationsmodelle einfügen.

Für die detaillierten Regulierungsvorschläge verweisen wir auf den Abschnitt 3.5.

5.2.3 Zum Konzept Government as a Plattform (GaaP)

Die Befähigung zur Teilhabe setzt voraus, dass das Internet auch als Vertrauensraum funktioniert, in dem Menschen und Unternehmen mit vertrauenswürdigen Mitteln ihre Identität und wichtige Eigenschaften nachweisen können. Zur Grundversorgung im digitalen Raum gehört deshalb, dass Menschen und Unternehmen sich ausweisen können. Zwar gibt es zahllose elektronische Identitäten, doch deren Einsatz ist eng begrenzt, weshalb Menschen und Unternehmen viele von ihnen verwalten müssen. Darüber hinaus sind die Kontrolle und Selbstbestimmung dieser elektronischen Identitäten stark eingeschränkt. Wir empfehlen daher ein eID-Ökosystem von SSI Zertifikaten zu etablieren, staatlich verankert, aber mit umfassender Beteiligung von Privatwirtschaft und Zivilgesellschaft.

5.3 Fazit und Ausblick

Das **Schichtenmodell** mit acht Ebenen der digitalen Souveränität, welches an dieser Stelle herangezogen wurde, hilft in einem weitgehend noch unerforschten Gebiet zwischen Service Public und digitaltechnologischer Entwicklung Ordnung zu schaffen. Mit dem politischen Konzept der digitalen Souveränität wurde hier der Versuch gemacht, die Lücke zu schliessen, die sich bei der Betrachtung digitaler Güter und Dienstleistungen eröffnet hat. Die übliche Begründung für ein staatliches Angebot (unzureichendes flächendeckendes Angebot für alle Bevölkerungsschichten in guter Qualität und zu angemessenen Preisen) kann für digitale Güter mit Ausnahme der Schicht 2 (Kommunikationsinfrastruktur) nicht herangezogen werden. Der Nachteil des Schichtenmodells besteht allerdings darin, dass es von der Absicht sehr weit gefasst ist und neben der Lösung von staatlichen Angeboten (bzw. digitalen Infrastrukturen) auch reine Regulierungsvorhaben als Lösungen einschliesst. Damit wird aber das engere Feld des Service Public verlassen. Aus diesem Grund sind viele digitaltechnologische Herausforderungen im Zusammenhang mit monopolitischer Plattformbildung kein Marktversagen, aber möglicherweise ein Versagen des Rechts, da es innovationshemmend wirken kann. Die Tabelle 2 (S. 36) versucht, die Herausforderungen auf die Schweiz zu beziehen, diese Überlegungen müssten aber noch validiert werden.

Aus **ökonomischer Perspektive** sollte mit dem Konzept der Datenallmende vertieft abgeklärt werden, unter welchen Bedingungen der Staat eine direkte oder indirekte Beteiligung an der Datenallmende

übernehmen soll. Eine systematische Analyse für Deutschland und die Europäische Union liegt vor, doch steht nicht fest, in welchen Sektoren ein Nettoeffekt auftreten wird. Deshalb, so folgern Bertschek et al. (Bertschek et al., 2021), müsste für einzelne Märkte jeweils spezifisch analysiert werden, «ob bei der Einrichtung einer Datenallmende tatsächlich ein ökonomischer Mehrwert zu erwarten ist, und welche Daten genau mit welchen Nutzerinnen und Nutzern zu teilen sind, um diesen Mehrwert zu erreichen.» (Bertschek et al., 2021). An dieser Stelle wurden mit Mobilität und Gesundheit zwei Beispiele erwähnt, welche als «Experimentierräume» aufzeigen könnten, ob eine Datenteilung sich volkswirtschaftlich und gesellschaftlich im Hinblick auf die Generierung von Public Value positiv auswirken wird. Möglich wäre ein stufenweises Vorgehen: zuerst freiwillige Datenteilung, anschliessend eine vom Staat finanziell unterstützte Datenteilung, schliesslich eine Datenteilungspflicht. Solche Untersuchungen sind deshalb wichtig, weil für eine staatliche Intervention letztlich volkswirtschaftliche Gesamteffekte nachgewiesen werden müssen.

Die in diesem Bericht aufgezeigten Herausforderungen eines zukünftigen Digitalen Service Public hat die Frage der **Governance**, also der übergreifenden Gestaltung und Führung der digitalen Transformation, nicht berücksichtigt. Gerade weil die Herausforderungen in der «Digitalen Gesellschaft» über den Nationalstaat hinausgreifen (siehe etwa die global agierenden Hyperscaler), ist eine Regulierung oder eine staatliche Bereitstellung allfälliger digitaler Infrastrukturen vermutlich nur im Verbund mit der Europäischen Union oder mit anderen internationalen Regierungsorganisationen zu bewältigen. Eine weitere Herausforderung bezüglich der Governance besteht darin, dass sich eine übergreifende IT-Governance in der föderalen Schweiz mit erheblichen Schwierigkeiten konfrontiert sieht, wie die Erfahrungen aus vergangenen zwei Dekaden im E-Government aufzeigen. In internationalen Monitorings schneidet die Schweiz eher schlecht ab, das Beispiel der Gesetzgebung Elektronisches Patientendossier beispielswiese ist primär ein Problem mangelnder IT-Governance. Was immer ein Digitaler Service Public einst für Gebiete erfassen wird, entscheidend für eine erfolgreiche Umsetzung wird die Herausbildung einer geeigneten Governance über die föderalen Ebenen hinweg sein. Ausserdem verlangt eine solche Governance den Einbezug der Bürgerinnen und Bürger (partizipative Ansätze), um die Risiken des politischen Scheiterns zu minimieren, wie die eID Vorlage im Referendum aufgezeigt hat.

6 Glossar

Cloud	Modell der Verarbeitung von → *Daten* mit dem bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (bspw. Netze, Server, Speichersysteme, Anwendungen und Dienste) zugegriffen werden kann. Diese können schnell und mit minimalem Verwaltungsaufwand bzw. geringer Serviceprovider-Interaktion zur Verfügung gestellt werden.
Daten	In der Informatik und Datenverarbeitung versteht man Daten als (maschinen-) lesbare und -bearbeitbare, in der Regel digitale Repräsentation von Information.
Dateninfrastruktur	Die notwendigen technischen und organisatorischen Systeme und Strukturen, um → *Daten* auszutauschen und nutzbar zu machen. Durch die Nutzung der Dateninfrastruktur durch Datengebende, Datennutzende sowie Intermediäre entstehen → *Datenräume*.
Datenräume	Technische und organisatorische Struktur, welche Bereitstellung, Austausch und Bezug von → *Daten* aus verschiedenen Quellen und von verschiedenen Akteuren ermöglicht und regelt. Oftmals sektorenspezifisch organisiert und durch Zweck, klare Regeln und Standards definiert.
Digitale Güter	Digitale Güter sind Güter, welche aus digitalen Daten bestehen. Sie weisen ähnliche Eigenschaften auf wie öffentliche Güter (Nutzung ist nicht abhängig von der Anzahl Nutzenden, der Konsum ist nicht-rival) aus. Im Unterschied zu öffentlichen Gütern kann man allerdings die Nutzung digitaler Güter ausschliessen (z.B. über Lizenzen). Digitale Güter weisen Skalen- und Netzwerkeffekte auf.
Digitale Plattform	Digitale Plattformen können definiert werden als Produkte, Dienstleistungen oder Technologien, die als Basis für eine Vielzahl von Firmen dienen, um komplementäre Produkte, Dienste und Technologien anzubieten.
Digitale Souveränität	Unter digitaler Souveränität wird die kollektive (Staat) als auch die individuelle Handlungsfähigkeit in einer digitalen Welt verstanden. Individuen, Unternehmen und die Gesellschaft als Ganzes sollen über ihr Handeln im digitalen Raum selbst bestimmen können. Oft wird auch der Begriff «digitale Selbstbestimmung» gebraucht und mit den Konzepten «Datensouveränität» und «informationelle Selbstbestimmung» zusammen verwendet (Pohle, 2021) Üblicherweise wird in Bezug auf die kollektive Ebene mehr von digitaler Souveränität gesprochen, auf individueller mehr von digitaler Selbstbestimmung. Das

	Individuum soll das Recht und/oder die Möglichkeit und Fähigkeit haben, grundsätzlich selber über Preisgabe, Sammlung und Verwendung → personenbezogener Informationen/*Daten* zu bestimmen sowie Kontrolle über ihr "digitales Double" zu haben.
Government as a Platform (GaaP)	Gemäss der OECD kann von "Government as a Platform" gesprochen werden, wenn eine Regierung als Plattform für die Erfüllung der Bedürfnisse der Nutzer fungiert, indem sie klare und transparente Quellen für Leitlinien, Werkzeuge, → *Daten* und Software bereitstellt, die es Teams ermöglichen, nutzerorientierte, konsistente, nahtlose, integrierte, proaktive und sektorübergreifende Dienstleistungen zu erbringen. GaaP kann entweder ein Ökosystem sein oder ein Marktplatz, oder eine Neudefinition der Beziehungen zwischen Einwohner*innen und Staat.
Hyperscaler	Skalierbare → *Cloud*-Computing-Systeme, in denen eine sehr grosse Zahl an Servern in einem Netzwerk verbunden ist. Die Zahl der genutzten Server kann je nach Bedarf vergrössert oder verkleinert werden. Dominierende Anbieter sind Amazon (Amazon Web Services (AWS), Microsoft (Azure), Google (Google Cloud Platform, CCP) und IBM, daneben von Bedeutung auch in China die Alibaba Cloud.
Open Source	Als Open Source (aus englisch open source; wörtlich offene Quelle) wird Software bezeichnet, deren Quelltext öffentlich und von Dritten eingesehen, geändert und genutzt werden kann.
Plattformisierung	Unter Plattformisierung wird der Prozess verstanden, wonach in der Digitalwirtschaft aufgrund von Netzwerkeffekten («alle meine Freunde sind bei Facebook») eine Tendenz zu einer marktbeherrschenden Stellung besteht.
Service Public	Ein unscharfer normativer Begriff in der politischen Landschaft der Schweiz, unter dem Dienstleistungen von allgemeinem (wirtschaftlichen) Interesse verstanden werden. Die offizielle, in Politik und Verwaltung verwendete Definition lautet: «Service Public umfasst eine politisch definierte Grundversorgung mit Infrastrukturgütern und -dienstleistungen, welche für alle Bevölkerungsschichten und Regionen des Landes nach gleichen Grundsätzen in guter Qualität und zu angemessenen Preisen zur Verfügung stehen sollen». In Deutschland ist der Begriff Daseinsvorsorge geläufig

7 Literaturverzeichnis

Arthur, W. B. (1989). Competing Technologies, Increasing Returns, and Lock-In by Historical Events. *The Economic Journal*, *99*(394), 116. https://doi.org/10.2307/2234208

BAKOM. (2021a). *Bericht Digitaler Service public - Beitrag Medien: unveröffentlicht*.

BAKOM. (2021b). *Was ist «Service public»? unveröffentlicht*.

BAKOM. (2021c). *Zusammenfassung Workshop Digitaler Service Public 2(9. und 30. April 2021): unveröffentlicht*. o.O.

Becker, M. (2017). Ein Recht auf datenerhebungsfreie Produkte. *JuristenZeitung*, *72*(4), 170. https://doi.org/10.1628/002268817X14845656323252

Bernard, L., Brauner, J., Mäs, S. & Wiemann, S. (2019). Geodateninfrastrukturen. In M. Sester (Hrsg.), *Geoinformatik* (S. 91–122). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-662-47096-1_66

Bertschek, I., Bonin, H., Kühling, J., Thüsing, G. & Wenzel, T. (2021). Entwicklung eines Konzepts zur Datenallmende: Expertise. *0174-4992*, *FB581*, 98. https://www.ssoar.info/ssoar/handle/document/75708

Biaggini, G. (2017). *BV: Kommentar : Bundesverfassung der Schweizerischen Eidgenossenschaft* (2. Aufl.). *Navigator.ch*. Orell Füssli Verlag.

Blenn, N. & Kuipers, F. (2017, 9. Juni). *LoRaWAN in the Wild: Measurements from The Things Network*. https://arxiv.org/pdf/1706.03086

Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.). (2018). *„Eigentumsordnung "für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive.*

Busch, C. (2021). *Regulierung digitaler Plattformen als Infrastrukturen der Daseinsvorsorge.*

Clement, R. & Schreiber, D. (2013). *Internet-Ökonomie*. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-36719-9

Collova, P., Marti, M., Schwarz, D., Wäspi, F. & Wenger, N. (2022). *Vertrauenswürdige Datenräume unter Berücksichtigung der digitalen Selbstbestimmung: Studie zu zentralen Herausforderungen, Grundprinzipien und Voraussetzungen, konkreten Beispielen sowie Kernelementen eines Modells vertrauenswürdiger Datenräume im Auftrag des BAKOM*. Bern. Berner Fachhochschule Wirtschaft. https://www.newsd.admin.ch/newsd/message/attachments/70836.pdf

Daubitz, S. (2021). Teilhabe und Öffentliche Mobilität: Die Rolle der Politik. In O. Schwedes (Hrsg.), *Öffentliche Mobilität: Voraussetzungen für eine menschengerechte Verkehrsplanung* (S. 77–101). Springer VS. https://doi.org/10.1007/978-3-658-32106-2_4

Durumeric, Z., Li, F., Kasten, J., Amann, J., Beekman, J., Payer, M., Weaver, N., Adrian, D., Paxson, V., Bailey, M. & Halderman, J. A. (11052014). The Matter of Heartbleed. In C. Williamson, A. Akella & N. Taft (Hrsg.), *Proceedings of the 2014 Conference on Internet Measurement Conference* (S. 475–488). ACM. https://doi.org/10.1145/2663716.2663755

Ecoplan. (2019). *Daten als Infrastruktur für multimodale Mobilitätsdienstleistungen: Zuhanden des Bundesamtes für Landestopografie swisstopo.*

Erass, C. (2020). Droit public : questions choisies / Rechtliche Probleme staatlicher Forschungsförderung. In V. Boillet (Hrsg.), *Le droit public en mouvement* (S. 191–211).

Europäische Kommission. (2015). *Creating value through open data: study on the impact of re use of public data resources*. Publications Office. https://op.europa.eu/en/publication-detail/-/publication/51ec011a-e13b-11e6-ad7c-01aa75ed71a1/language-en https://doi.org/10.2759/328101

Europäische Kommission. (2020a). *The Digital Markets Act: ensuring fair and open digital markets*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en

Europäische Kommission. (2020b). *The Digital Services Act: ensuring a safe and accountable online environment*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

Früh, A., Braun Binder, N. & Schibli, R. (2022). Data Governance für Smart Mobility aus rechtlicher Perspektive. *sui generis.* Vorab-Onlinepublikation. https://doi.org/10.21257/sg.200

Gonser, N. & Gundlach, H. (2020). Public Value. In J. Krone & T. Pellegrini (Hrsg.), *Handbuch Medienökonomie* (S. 1563–1589). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-09560-4_48

Greenstein, S. (1997). Lock-in and the Costs of Switching Mainframe Computer Vendors: What Do Buyers See? *Industrial and Corporate Change*, *6*(2), 247–273. https://doi.org/10.1093/icc/6.2.247

Guyan, P. (2018). Zugänglichkeit von schweizerischen Gerichtsentscheiden im Internet. *Justice - Justiz - Giustizia*(2), 1–5.

Hildén, J. (2021). Mitigating the risk of US surveillance for public sector services in the cloud. *Internet Policy Review*, *10*(3). https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud

Hitz-Gamper, B. S. & Stürmer, M. E. (2021, 17. September). *Daten in OpenStreetMap integrieren – ein Leitfaden für Dateninhaber.* Forschungsstelle Digitale Nachhaltigkeit. https://boris.unibe.ch/159438/

Hürlimann, D. & Kettiger, D. (2021). *Anonymisierung von Urteilen*. Helbing Lichtenhahn Verlag. https://www.helbing.ch/annot/44433A484C567C7C353538387C7C504446.pdf https://doi.org/10.46455/Helbing_Lichtenhahn/978-3-7190-4270-7

Johnson, J. P. (2002). Open Source Software: Private Provision of a Public Good. *Journal of Economics & Management Strategy*, *11*(4), 637–662. https://doi.org/10.1111/j.1430-9134.2002.00637.x

Kagermann, H., Streibich, K.-H. & Suder, K. (2021). European Public Sphere. Gestaltung der digitalen Souveränität Europas (acatech IMPULS).

Keane, M. & Yu, H. (2019). Communication, Culture, and Governance in Asia | A Digital Empire in the Making: China's Outbound Digital Platforms. *International Journal of Communication*, *13*(0), 18. https://ijoc.org/index.php/ijoc/article/view/10995

Keller, P. & Tarkowski, A. (2021). Digital Public Space – A missing policy frame for shaping Europe's digital future. *Open Future*. https://openfuture.pubpub.org/pub/digital-public-space-policy-frame/release/1

Kellerhals, A. (2018). Open Government Data – ein Beitrag zur Digitalisierung von Demokratie und öffentlicher Verwaltung. *Yearbook of Swiss Administrative Sciences*, *9*(1), 66. https://doi.org/10.5334/ssas.120

Kiener, R., Kälin, W. & Wyttenbach, J. (2018). *Grundrechte* (3. Aufl.). *Stämpflis juristische Lehrbücher*. Stämpfli Verlag.

Knieps, G. (2007). *Netzökonomie: Grundlagen — Strategien — Wettbewerbspolitik*. *SpringerLink Bücher*. Gabler. https://doi.org/10.1007/978-3-8349-9231-4

Knobel, I., Fegert, M. & Detreköy, N. (Dezember 2020). *Health Data Governance: What's in it for Switzerland?* foraus. https://www.foraus.ch/wp-content/uploads/2020/12/20201216_IDH_DE_WEB-1.pdf

Lütjens, K., Radde, M., Liedtke, G., Maertens, S., Standfuss, T., Scheier, B. & Viergutz, K. (2018). Innovationen im Zuge der Digitalisierung des Personenverkehrs. *Wirtschaftsdienst*, *98*(7), 512–518. https://doi.org/10.1007/s10273-018-2324-5

Mause, K. (2018). Daseinsvorsorge. In R. Voigt (Hrsg.), *Handbuch Staat* (S. 415–421). Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-20744-1_37

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology*. Galthersburg. NIST.

Müller, G. & Vogel, S. (2014). *Rechtsgutachten zur verfassungsrechtlichen Zulässigkeit der Randnutzung von Software im Verwaltungsvermögen, insbesondere der Veröffentlichung und Verbreitung von Open-Source-Software durch Träger von Bundesaufgaben*. Erlinsbach/Fällanden. https://www.news.admin.ch/NSBSubscriber/message/attachments/37015.pdf

Neu, C. (2009). Daseinsvorsorge – eine Einführung. In C. Neu (Hrsg.), *Daseinsvorsorge* (S. 9–19). VS Verlag für Sozialwissenschaften. https://doi.org/10.1007/978-3-531-91876-1_1

OECD. (2020). *The OECD Digital Government Policy Framework: Six Dimensions of a Digital Government* (OECD Public Governance Policy Papers). https://www.oecd-ilibrary.org/governance/the-oecd-digital-government-policy-framework_f64fed2a-en https://doi.org/10.1787/f64fed2a-en

Otto, B. & Burmann, A. (2021). Europäische Dateninfrastrukturen. *Informatik Spektrum*, *44*(4), 283–291. https://doi.org/10.1007/s00287-021-01386-4

Piolino, M. (2021). *Die Staatsunabhängigkeit der Medien. sui generis*. sui generis Verlag für Open-Access-Publikationen. https://books.google.ch/books?id=6HlhEAAAQBAJ

Pohle, T. (2021). Digitale Souveränität - Von derKarriere eines einenden und doch problematischen Konzepts. In C. Piallat, J. Pohle & T. Thiel (Hrsg.), *Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt.*

Poledna, T., Schlauri, S. & Schweizer, S. (2017). *Rechtliche Voraussetzungen der Nutzung von Open-Source-Software in der öffentlichen Verwaltung, insbesondere des Kantons Bern*. Carl Grossmann.

Reiners, W. (2021). Die Digitalisierungsstrategie der Europäischen Union – Meilensteine und Handlungsfelder zwischen digitaler Souveränität und grüner Transformation. *integration*, *44*(4), 266–286. https://doi.org/10.5771/0720-5120-2021-4-266

Renda, A. (2020). Making the digital economy “fit for Europe”. *European Law Journal*, *26*(5-6), 345–354. https://doi.org/10.1111/eulj.12388

Rötzer, H. (2020). Die helvetische elektronische Identität. *SocietyByte (Wissenschaftsmagazin der Berner Fachhochschule)*.

Sahay, S. (2019). Free and open source software as global public goods? What are the distortions and how do we address them? *The Electronic Journal of Information Systems in Developing Countries*, *85*(4), e12080. https://doi.org/10.1002/isd2.12080

Schallbruch, M. (2022). *Risiken der Cybergesellschaft beherrschen. Ein Auftrag an Staat und Politik – Deutschland und die Welt 2030*. https://deutschland-und-die-welt-2030.de/de/beitrag/risiken-der-cybergesellschaft-beherrschen-ein-auftrag-an-staat-und-politik/

Schlauri, S. (2010). *Network Neutrality: Netzneutralität als neues Regulierungsprinzip des Telekommunikationsrechts* [, University of Zurich]. www.zora.uzh.ch. https://www.zora.uzh.ch/id/eprint/36715/

SDA. (2015). *Bern: Nationalrat versenkt neuen Grundversorgungsartikel.* RRO Radio Rottu Oberwallis. https://www.rro.ch/cms/?page=news&detail=80538

Stuermer, M., Krancher, O. & Myrach, T. (2017). When the Exception Becomes the Norm. In R. Baguma (Hrsg.), *Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance* (S. 43–46). ACM. https://doi.org/10.1145/3047273.3047329

Sturn, R. (2021). Der Staat heute: Marktversagen und die Voraussetzungen öffentlicher Handlungsfähigkeit. *Wirtschat und Gesellschaft*, *47*(1), 15–40.

Swiss Data Alliance. (2021). *Der europäische Datenraum aus Schweizer Sicht: Whitepaper.*

UVEK & EDA. (2022). *Schaffung von vertrauenswürdigen Datenräumen basierend auf der digitalen Selbstbestimmung: Bericht des UVEK und des EDA an den Bundesrat*. Bern. https://www.newsd.admin.ch/newsd/message/attachments/70835.pdf

van Dijck, J. (2021). Platform, Power, Public Counter-Power: Governing Platformization in Europe. *The Pontifical Academy of Social Sciences*. http://www.pass.va/content/scienzesociali/en/publications/studiaselecta/changing_media/van_dijck.pdf

Wolking, C. (2021). Öffentliche Mobilität und neue Mobilitätsdienstleistungen – Rahmenbedingungen und Gestaltungsperspektiven. In O. Schwedes (Hrsg.), *Öffentliche Mobilität: Voraussetzungen für eine menschengerechte Verkehrsplanung* (S. 105–138). Springer VS. https://doi.org/10.1007/978-3-658-32106-2_5

Xiaoguo Zhu, K. & Zhizhong Zhou, Z. (2011, 16. Juni). *Research Note—Lock-In Strategy in Software Competition: Open-Source Software vs. Proprietary Software | Information Systems Research.*